Facultad de Ingeniería

Ingeniería de Redes y Comunicaciones

Tesis:

“Propuesta de un Diseño del Protocolo Secure SD-WAN para garantizar el balanceo de carga en la comunicación de L2L de forma inteligente y segura para la empresa Cencosud S.A. Lima 2020”

Héctor Dante Britto Infantas
Rubén Isidro Vilcapoma Enrique

Para obtener el Título Profesional de Ingeniero de Redes y Comunicaciones

ASESOR (A): MBA ING.CIP. Roxana Janet Quiroz Valenzuela

Lima – Perú

2020

Dedicatoria

Este trabajo está dedicado a Dios, por darme la oportunidad de llegar hasta esta instancia de mi vida, asimismo a toda mi familia comprendida por mis padres Don Héctor y Doña Delia y mi hermana Pamela por brindarme la fuerza para continuar en este sueño y no rendirme antes las adversidades, por inculcarme los valores desde casa y ser un hombre de bien con muchas aspiraciones y sueños. Dedico también y de una forma muy especial a mis sobrinos Luciano y Alanna por mostrarme lo simple que puede ser la vida por darme ese ánimo mediante su alegría y carisma que me hace ver aspectos muy diferentes de la vida y del propósito como el legado que quiero dejar en este mundo.

Hector Dante Britto Infantas

Este trabajo está dedicado en primer lugar a Dios, por darme la vida. Asimismo, a mi madre Ana María, por demostrar su apoyo incondicional. A mi padre Max por incentivarme a emprender este camino, y para toda mi familia por estar dispuestos a escuchar mis opiniones y ayudarme en cualquier espacio de mi vida, sin su apoyo no lo hubiera logrado.

Rubén Isidro Vilcapoma Enrique

Agradecimiento

Agradezco a mi asesora de tesis Ing. Roxana Quiroz Valenzuela, como a mis profesores dentro de mi proceso universitario por su paciencia, tiempo y la enseñanza brindada; el cual, ha sido muy satisfactorio durante mi incursión universitaria y crecimiento personal como profesional. A mis compañeros por el apoyo y ánimos a seguir prosperando y poniéndole mucho corazón y fuerza para continuar y culminar mi carrera de Ingeniería de Redes & Comunicaciones.

Agradezco a mi familia por su sacrificio y darme la oportunidad de culminar mis estudios y creer en mis sueños como la confianza en todas mis aptitudes, por regalarme el cariño y enseñarme lo que es el significado de una verdadera familia.

Hector Dante Britto Infantas

Agradezco a mi asesora de tesis Ing. Roxana Quiroz Valenzuela por la enseñanza que me ha brindado, también a mi madre Ana María por su confianza y apoyo, ella sin duda me ha demostrado su amor en mi vida, corrigió mis errores y celebró mis victorias.

Para mi padre Max, él siempre ha sido la fuerza impulsadora de mi vida. Sé que está orgulloso de quien soy. Estoy especialmente agradecido a mis tíos Juan y Norma por su compresión. En el proceso de desarrollo de este proyecto, rindo homenaje a todas las personas que me han apoyado.

Rubén Isidro Vilcapoma Enrique

Índice General

Lista de Figuras

Lista de Tablas

Lista de Anexos

Introducción

En la actualidad, los supermercados peruanos continúan su evolución positiva durante cada año, ofreciendo nuevos establecimientos de ventas, lo cual incrementa su participación en el sector mayorista y minorista a nivel nacional. Asimismo, el crecimiento de los supermercados va de la mano con el desarrollo de las tecnologías y de las Telecomunicaciones. En este Contexto, resulta necesario garantizar la operatividad de los enlaces de transmisión de datos (L2L) e Internet para proveer la continuidad del negocio.

El objetivo general es garantizar el balanceo de carga en la comunicación de L2L de forma inteligente y segura para la empresa Cencosud S.A.

Al pasar el tiempo la demanda del sector de telecomunicaciones corporativo exige mayores velocidades, eficiencia, eficacia y tiempo de respuesta rápida ante alguna avería o desastre que evite la indisponibilidad del servicio. Por ende, la importancia de la propuesta del protocolo Secure SD-WAN, permitirá administrar la red WAN de una mejor manera logrando optimizar el rendimiento de las redes, como el aumento de la agilidad en las operaciones de las entidades, beneficiando a la producción del negocio.

El protocolo Secure SD-WAN contiene varios aportes; uno de ellos es el balanceo de enlaces de forma inteligente, a través de esta función, se logrará optimizar y simplificar la gestión de los sistemas informáticos. Del mismo modo, la solución contribuirá mejorar la experiencia del usuario sobre el uso de la red de datos, que garantizará mejor rendimiento, rapidez y seguridad distribuida en la comunicación entre las sucursales de la empresa Cencosud S.A.

El proyecto de tesis está compuesto por 6 capítulos. En el capítulo 1, se verá los aspectos generales constituido por los antecedentes del problema y los objetivos generales y específicos. En el capítulo 2, se argumentará el marco teórico con bases conceptuales de las tecnologías que formará parte del documento de tesis. En el capítulo 3, se planteará el planteamiento de la Metodología de investigación. Asimismo, en el capítulo 4, se desarrollará la Metodología para la implementación sobre la propuesta de la investigación de tesis. En el capítulo 5, se reflejará los resultados de la solución desarrollada a través de los instrumentos de mediciones. En el capítulo 6, se analizará los costos y beneficios sobre los aspectos administrativos, económicos y el análisis de sensibilidad, para determinar el financiamiento de la presente investigación y finalmente, daremos nuestras conclusiones y recomendaciones.

CAPÍTULO I

Aspectos Generales

1.1. Antecedentes del problema

En referencia a los supermercados peruanos es preciso indicar que continúan en su evolución positiva durante el año 2020, según el reporte oficial del (Banco Scotiabank del Perú, 2019), las ventas del canal minorista moderno que incluyen hipermercados, supermercados y tiendas de descuentos alcanzaron el monto de S/. 5,101 millones de nuevo sol creciendo cerca del 7% en el año 2019 y se estima crecer para el año 2020.

Asimismo, en Perú, la división de supermercados de Cencosud S.A. Aumentó sus ventas de 5 % a 8.5% durante el periodo anual del 2019 como resultado por la continuidad de estrategias de ventas promocionales, la maduración de tiendas inauguradas en años previos y planificadas para los próximos años. Tal como se muestra en la Figura 1.

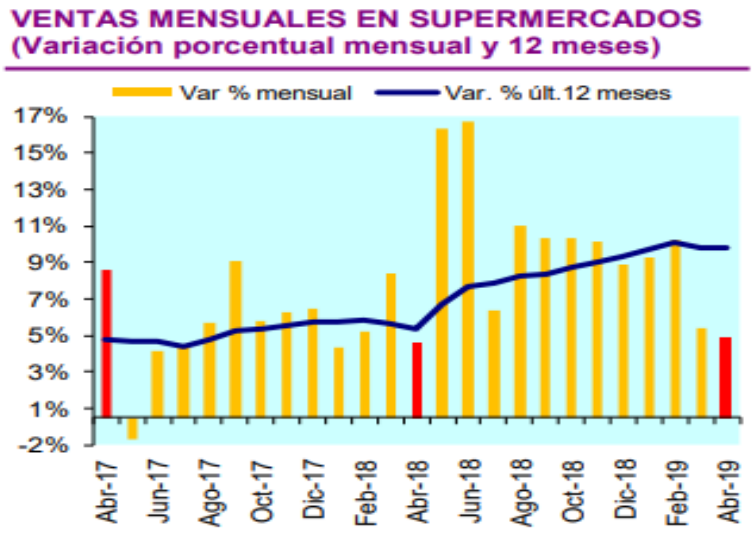


Figura 1. Ventas Mensuales en Supermercados

Fuente: (Scotiabank, 2019)

En la actualidad, Cencosud S.A. en el sector de las Telecomunicaciones tiene desplegado el servicio de interconexión de sedes bajo la arquitectura de red MPLS[1]. Por lo tanto, los supermercados están intercomunicados entre si mediante el esquema de L2L[2]. Lo que permite establecer las transacciones de cajas, acceso al sistema de intranet[3] y envió de facturación electrónica. Por lo tanto, Cencosud S.A. cuenta con alta demanda en sus operaciones con relación a los sistemas informáticos. Es por ello, es vital su funcionamiento en todos los establecimientos de ventas.

La empresa cuenta con los siguientes puntos críticos:

- Puntos de ventas
- Cajeros
- Área de Almacén
- Área de Facturación

El día 24 de febrero del año 2020, el Gerente Regional de Cencosud S.A. Perú, presenció la inoperatividad de los sistemas informáticos en varios establecimientos de ventas, esto produjo pérdidas económicas por el tiempo de 3 horas generando un gran impacto al negocio. En relación con este tema, el área de Telecomunicaciones de Cencosud S.A. identificó el congestionamiento de tráfico en el enlace de L2L de la Oficina Central que ocasionó la falla de las operaciones en todas las sucursales. Es por ello, qué el caso fue escalado al proveedor de servicios, que diagnosticaron el uso no adecuado del ancho de banda de la Oficina Central que garantiza la comunicación de datos en todas las tiendas de la empresa.

---

[1] **MPLS:** Conmutación de etiquetas multiprotocolo, es un estándar para comunicación de datos.
[2] **L2L:** Red Lan to Lan (red de área local) que comparte una línea de comunicación.
[3] **Intranet:** Red informática interna de una organización.

Por todo lo explicado anteriormente se concluye que Cencosud S.A. Perú, no cuenta con un diseño de alta disponibilidad en los enlaces de L2L que otorgue la distribución adecuada del ancho de banda. En efecto ante la presencia de congestionamiento de tráfico o avería de fibra óptica conllevaría a un gran impacto negativo en la producción.

De tal manera vista la necesidad de los problemas en el diseño de la red, se necesita diseñar una solución que resuelva la problemática que presenta la empresa en su ambiente de Telecomunicaciones. Por tal razón Cencosud S.A. decidirá invertir en una solución que garantice la disponibilidad del servicio ante el impacto de una avería de gran escala y que ofrezca un valor agregado único que permita distribuir la carga para optimizar los recursos de red que proporcione un acceso rápido y seguro a los sistemas informáticos de la empresa.

Actualmente para las comunicaciones, sobre todo en el sector corporativo es de carácter fundamental contar con soluciones de balanceo de carga que permita garantizar la disponibilidad de enlaces ante algún problema de tráfico de red o avería a nivel de proveedores de Internet, lo cual permita la continuidad del negocio.

En tal sentido, la demanda del sector de Telecomunicaciones exige mayores velocidades, eficiencia, eficacia y tiempo de respuesta rápida ante alguna falla de enlace que ocasione la indisponibilidad del servicio. Por ende, las tecnologías se han ido masificando y ofreciendo mejores soluciones en el mercado, desde el año 2020 se habla mucho del protocolo Secure[4] SD-WAN[5] en un enfoque definido por software inteligente que permitirá administrar la red WAN[6] que logrará optimizar y mejorar el rendimiento del

[4] **Secure:** Seguridad de red
[5] **SD-WAN:** Redes definidas por Software en una red de área amplia.
[6] **WAN:** Red de área amplia.

negocio como la agilidad de las operaciones de las entidades como la presencia de reposición del enlace ante alguna avería de medio óptico.

Por otro lado, se utilizarán enlaces de MPLS para garantizar la seguridad y la conectividad, lo que ya no es suficiente en un mundo donde las empresas compiten por adoptar aplicaciones y arquitecturas clouds. Tal como se muestra en el año 2020, SD-WAN está entrando con fuerza generando grandes cambios en el mundo de las redes WAN.

Tal como se muestra en la Figura 2 líneas abajo basado en el crecimiento de SD-WAN.

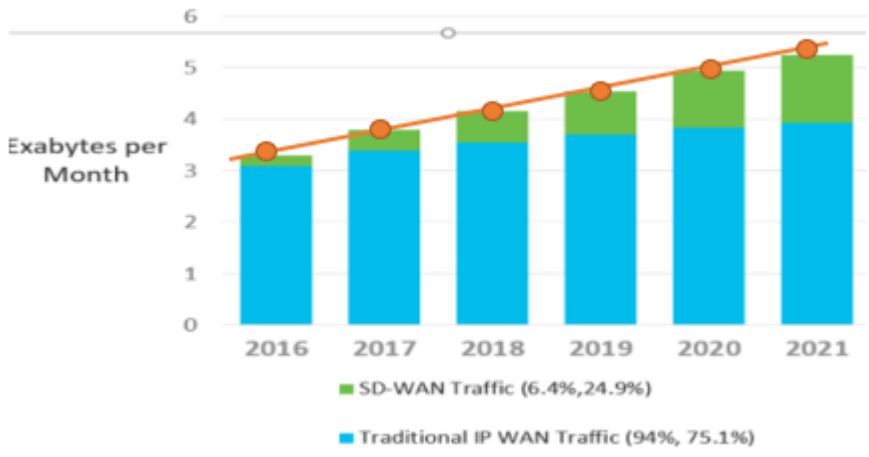


Figura 2. Crecimiento de SD-WAN

Fuente: (Gartner, 2020)

En los últimos 6 años se ha incrementado exponencialmente el tráfico de SD-WAN en los proveedores de servicios, siendo los rubros de e-commerce, bancos, cajas, universidades y supermercados brindando de esta manera una mejor experiencia al cliente.

1.2. Definición del Problema

No se cuenta con un diseño del protocolo Secure SD-WAN para garantizar el balanceo de carga en la comunicación de L2L de forma inteligente y segura para la empresa Cencosud S.A. Lima 2020.

1.3. Definición de los Objetivos

1.3.1. Objetivo General

Diseñar una propuesta del protocolo Secure SD-WAN para garantizar el balanceo de carga en la comunicación de L2L de forma inteligente y segura para la empresa Cencosud S.A. Lima 2020.

1.3.2. Objetivos Específicos

- Recopilar los datos de carga de la empresa Cencosud S.A. para diseñar el protocolo Secure SD-WAN.
- Determinar cómo contribuye la capacidad de red para el uso del balanceo de carga en la comunicación de L2L de forma inteligente y segura para la empresa Cencosud S.A.
- Realizar el monitoreo de los enlaces para medir el rendimiento en el balanceo de carga en la comunicación de L2L de forma inteligente y segura para la empresa Cencosud S.A.

1.4. Justificación de la Investigación

La presente investigación beneficiará a la empresa Cencosud S.A, en la disponibilidad de enlace, optimización de tráfico, seguridad integrada y simplificación en la operación de red, ofreciendo la continuidad del negocio, lo que mejorará la producción de la empresa brindándoles la mejor experiencia del servicio.

Asimismo, en el campo social, se concentrará en mejorar la experiencia del trabajador y los comensales al mantener una atención rápida por parte del usuario al disponer de acceso continuo, óptimo y de alta disponibilidad con niveles de servicio predecibles.

El protocolo Secure SD-WAN ayudará en lo económico a no realizar grandes gastos de enlaces dedicados, ya que se tiene un punto a favor en el tema de integración de seguridad para la comunicación en la nube y balanceo inteligente usando el medio de internet. Por consiguiente, ofrece un diseño sencillo y práctico compatibilidad con las redes actuales.

CAPÍTULO II

Marco Teórico

2.1. Estado de la Cuestión

Actualmente, el sector corporativo vive una época de alta competencia y demanda, por ello, su visión se enfoca en ofrecer un servicio de calidad al cliente. En efecto es de carácter fundamental contar con soluciones de telecomunicaciones que permitan garantizar la disponibilidad de las comunicaciones sobre los servicios de Internet y enlaces dedicados soluciones que estén dispuestos a proveer un alto rendimiento, velocidad, eficiencia, eficacia, integridad, disponibilidad y seguridad de sus infraestructuras tecnológicas. Dentro de este marco las tecnologías han crecido exponencialmente y se han ido masificando en el mercado saliendo nuevas soluciones que ofrecen reforzar estos puntos y optimizar las telecomunicaciones del sector corporativo. Bajo esta información, es muy importante que los ingenieros de Networking estén preparados y capacitados para analizar, diagnosticar, afrontar, recomendar e implementar y buscar mejorar los puntos de fallos que ocurra dentro de las infraestructuras TICs a través de las nuevas soluciones de TI.

En los viejos tiempos, había que recurrir a mapas de papel, ahora vivimos en una era de información donde influye la tecnología y a través de su ayuda se puede evitar los tipos de problemas que ocurren en la actualidad como el rendimiento, velocidad y seguridad en las redes e infraestructura de TICs por ejemplo enlaces de internet congestionados, latencias y variación del paquete que pueda ocasionar una falla en la red (Fortinet, 2019).

En los últimos años las redes de datos de área local bajo una arquitectura de red tradicional se han vuelto más complejas y robustas debido a los nuevos requerimientos de los servicios de redes, tales como Big Data, colaboración e Internet de las cosas donde cada dispositivo de red cumple una función específica, la red tradicional presenta las siguiente inconvenientes: falta de escalabilidad, congestionamiento de red, inconsistencias de la información , falta de disponibilidad, falta de seguridad, etc. La arquitectura de las Redes Definidas por Software, en ingles Software Defined WAN (SD-WAN), supera estas problemáticas ya que, mediante el uso de sus algoritmos, optimiza la gestión de la red y su rendimiento independientemente de los enlaces de internet o enlaces dedicados. SD-WAN es una arquitectura de red flexible y automatizada abierta a nuevas posibilidades futuras (MEJIA, 2018)

Los nuevos modelos de negocios exigen un nuevo de modelo de red WAN que este dispuesto afrontar y abordar los desafíos actuales de las áreas de TI. Este nuevo método brinda conectividad de alta velocidades, optimización y un control del ancho de banda para su mejor uso y distribución para resolver problemas de congestionamiento y disponibilidad de red. SD-WAN ofrece eficiencia y garantiza un alto nivel de rendimiento para las aplicaciones críticas del sector corporativo, sin poner en riesgo la seguridad e integridad de los datos que viajan en la red (Cisco System, 2019),

2.2. Bases teóricas

2.2.1. Protocolo Secure SD-WAN.

2.2.1.1. Concepto de SD-WAN.

La gestión de la WAN siempre ha sido uno de los elementos más caros e inflexibles en la operación de una red empresarial, sin embargo, las nuevas características presentes en la tecnología SD-WAN han simplificado la administración con la aplicación de dispositivos de red programables, que permiten a los analistas ajustes de forma remota. Además, el sistema ejecutará automáticamente la elección de la mejor ruta de enrutamiento, disminuyendo costos y mejorando el rendimiento de las redes. Lo que hará que este servicio sea tan eficiente es precisamente su capa de software (SD, que significa Software Defined), que garantiza la calidad del servicio y la protección de datos de los enlaces de Internet, o transmisión de datos independientemente de su tipo (Ostec, 2018, pág. 1).

La SD-WAN, permitirá que el tráfico se envíe automáticamente a través del camino más adecuado de la WAN mediante sus algoritmos de forma inteligente, respetando las condiciones de seguridad, el costo de los circuitos y las exigencias de la calidad de los servicios. Esta calidad estará garantizada por la toma de decisión inteligente del software, que utilizará métricas de calidad de los enlaces, como el tiempo de respuesta, evitando que el encaminamiento se base sólo en el protocolo dinámico, al adoptar SD-WAN será posible usar enlaces de comunicación redundantes, administrados automáticamente por la aplicación, prácticamente eliminando la posibilidad de caídas y fallas en la comunicación, brindando equilibrio de carga de tráfico para utilizar múltiples enlaces WAN de manera efectiva. El uso efectivo de WAN se logrará utilizando varios algoritmos de equilibrio de carga, como el uso de ancho de banda, sesiones o enrutamiento consciente de la aplicación.

Otra característica importante de SD-WAN son las mediciones de calidad de enlace. Utilizando ping[7] o eco HTTP[8], se podrá determinar el porcentaje de latencia, jitter[9] o pérdida de paquetes para cada enlace, y seleccione dinámicamente enlaces basados en estas mediciones. Esto garantizará una alta disponibilidad para los negocios críticos aplicaciones (Ostec, 2018, pág. 1).

Tomaremos un ejemplo de un viaje por carretera. Todos aman un buen viaje por carretera, disfrutan de un viaje relajado y sin tránsito.

Figura 3. Protocolo SD-WAN Libre de Tráfico

Fuente: (Fortinet INC, 2020)

2.2.1.2. Secure SD-WAN.

La SD-WAN ofrece el manejo de aplicaciones comerciales, ahorro de costos y rendimiento para aplicaciones de software como un servicio en sus siglas SaaS, así como servicios de comunicación unificada. Sin embargo, la SD-WAN tiene sus propias

[7] **Ping:** Packet Internet Groper, es un comando de diagnóstico de conexión de red.
[8] **Http:** Protocolo de transferencia de hipertexto, permite las transferencias de información en la web
[9] **Jitter:** Fluctuación o variación de retardo de paquetes.

deficiencias, especialmente con respecto a la seguridad, es por ello qué Secure SD-WAN incluye las mejores capacidades de la industria de Next-Generation Firewalls, SD-WAN, enrutamiento avanzado y optimización de WAN, lo que brinda una transformación del borde de la WAN de redes basadas en la seguridad en una oferta unificada. La compañía Fortinet obtuvo la segunda calificación "Recomendada" consecutiva de NSS[10] Labs en la prueba de grupo de SD-WAN publicado por (Fortinet, 2019, pág. 1).

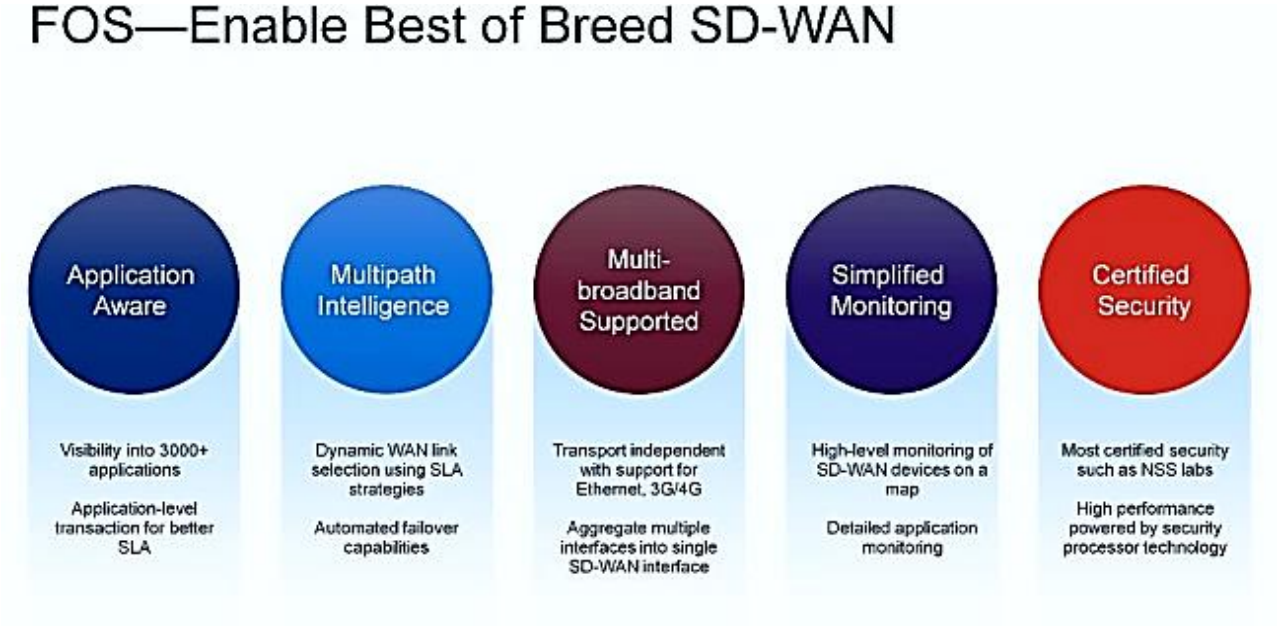


Figura 4. Beneficios de SD-WAN

Fuente: (Fortinet INC, 2020)

Según (Gartner INC, 2020) "estima que Fortinet tiene más de 21,000 clientes de WAN que se utilizan principalmente como UTM[11] / NGFW[12] para el mercado medio" (p.1). Fortinet se dirige al mercado SD-WAN con su producto estrella, FortiGate Secure

[10] **NSS:** Network security services (servicio de seguridad de red).
[11] **UTM:** Unified Threat Management, por su sigla en español (Gestión Unificada de Amenazas).
[12] **NGFW:** Next Generation Firewall, por su sigla en español (Nueva generación de Firewall).

SD-WAN, que aprovecha la sólida posición de Fortinet en la entrega de redes basadas en seguridad generalizada.

Figura 5. Cuadrante mágico de Gartner de seguridad SD-WAN

Fuente: (Gartner INC, 2020)

2.2.1.3. Regla de SD-WAN.

Las reglas SD-WAN le permitirán especificar qué tráfico desea enrutar a través de qué interfaz. Puedes configurar las reglas SD-WAN para elegir las interfaces de salida basadas en diferentes estrategias. Las reglas se evaluarán de la misma manera que las políticas de firewall: de

arriba a abajo, utilizando la primera coincidencia, puedes usar lo siguiente parámetros para que coincida con el tráfico:

- Dirección IP [13]origen
- Dirección IP de destino
- Número de puerto de destino
- Aplicación de firewall como destino
- Usuarios o grupos de usuarios.
- Tipo de servicio (ToS)

Las reglas SD-WAN ofrecen una gran flexibilidad cuando se compara el tráfico. Por ejemplo, puede enrutar el tráfico de Netflix desde usuarios autenticados específicos a través de un ISP[14], mientras enruta el resto del tráfico de Internet a través de otro ISP.

SD-WAN ofrece cuatro estrategias para seleccionar una o varias interfaces salientes: Manual, Mejor calidad, Costo más bajo (SLA[15]) y Maximizar el ancho de banda. Con la estrategia Manual, puede seleccionar la interfaz desde la que desea enviar el tráfico. Si el tráfico coincide Según los criterios de la regla, el tráfico saldrá de la interfaz seleccionada (Fortinet INC, 2019, pág. 64).

2.2.1.4. Aporte de SD-WAN en una Infraestructura red.

(Cisco System, 2019), considera que el diseño de redes WAN estaba limitado. A medida que las empresas adquieren aplicaciones basado en la nube en el entorno SaaS[16] /

[13] **IP:** Protocolo de Internet, es un número que identifica de forma única a un dispositivo en la red.
[14] **ISP:** Proveedor de Servicios
[15] **SLA:** Acuerdo de nivel de servicio
[16] **SaaS:** Software como servicio, permite a los usuarios conectarse a aplicaciones en la nube.

IaaS[17], su diseño WAN experimenta un aumento de tráfico al acceder a estas aplicaciones globalmente diversas. Estos nuevos modelos de negocio causan múltiples implicaciones para el área de TI[18]. La productividad de los empleados se ve afectada por los problemas de rendimiento de las aplicaciones. Al mismo tiempo, los gastos aumentan con el uso ineficiente de circuitos dedicados. El área de TI tiene el desafío de conectar múltiples tipos de usuarios, a través de múltiples tipos de dispositivos, a múltiples entornos de nube.

El protocolo SD-WAN, puede ofrecer múltiples métodos de balanceo inteligentes para dividir la carga del tráfico de dato. Asimismo, brinda protección contra amenazas, descarga eficiente y simplificación de la administración de la red WAN y los beneficios comerciales incluyen (p.1):

- Experiencia de la Aplicación:
  - Brinda alta disponibilidad en todas las aplicaciones críticas.
  - Múltiples enlaces activos-activos para todos los escenarios de red.
  - Enrutamiento dinámico del tráfico de las aplicaciones para impulsar una entrega eficiente.
- Seguridad Integra:
  - Políticas contextuales para aplicaciones con reforzamiento en tiempo real para problemas de red.
  - Protección integrada contra amenazas.
- Optimizado para la Nube:
  - Extienda perfectamente su WAN a múltiples nubes públicas.

[17] **IaaS:** Infraestructura como servicio, es una forma de computación en la nube
[18] **TI:** Tecnología de la información.

- Rendimiento optimizado en tiempo real para Office 365, Salesforce y otras aplicaciones SaaS críticas.
- Flujos de trabajo optimizados para plataformas en la nube como AWS[19] y Azure[20].

- Simplificación operativa y seguridad:
  - Panel de control único y centralizado para la configuración y gestión de red WAN, nube y seguridad.
  - Aprovisionamiento de cero toques basados en plantillas para todas las ubicaciones.
  - Reportes detallados de aplicaciones y de rendimiento WAN para análisis de negocio.

2.2.1.5. Beneficios del uso de SD-WAN.

La corporación (Cisco System, 2019), "afirma que SD-WAN puede beneficiar a los departamentos de TI con los siguientes puntos" (p.1):

- **Simplificar la gestión:**

  Como arquitectura de WAN centralizada y entregada en la nube, SD-WAN hace que sea fácil de escalar para miles de terminales, ya sea que estén en la sucursal, el campus o la nube. TI tiene la capacidad de automatizar la implementación de cero-toque globalmente, utilizando una sola interfaz de administración.

[19] **AWS:** Amazon web services
[20] **Azure:** Plataforma de Microsoft en la nube

- **Mejorar la experiencia del usuario:**

  La optimización de WAN ofrece un rendimiento óptimo de las aplicaciones en la nube, desde múltiples nubes hasta los usuarios en cualquier lugar. En caso de falla del enlace o degradación de este, el enrutamiento que reconoce la aplicación puede enrutar dinámicamente el tráfico entre circuitos dedicados y conexiones de Internet seguras para impulsar la entrega constante de aplicaciones críticas para el negocio.

- **Aumentar la seguridad:**

  La prevención de amenazas se aplica en el lugar correcto. La arquitectura SD-WAN presenta seguridad distribuida a nivel de sucursal. Los datos no tienen que viajar de vuelta a la sede central o al centro de datos para obtener una protección de seguridad avanzada (como un firewall, reforzamiento de DNS[21] o la prevención de intrusos).

2.2.2. Balanceo de Carga.

2.2.2.1. Métodos de balanceo de SD-WAN.

(Fortinet INC, 2019), considera que el equilibrio de carga SD-WAN utiliza métodos de distribución de tráfico que son similares a los utilizados por igual costo multi ruta (ECMP). El equilibrio de carga del enlace SD-WAN incluye un método de equilibrio más: volumen. Por defecto, el modo de equilibrio de carga está configurado en source-IP-based. Sin embargo, puede cambiar el equilibrio de carga modo a cualquiera de los siguientes (p.21):

[21] **DNS:** Domain Name System, por sus siglas en español (Sistema de nombres de dominio).

- **IP de origen (basado en IP de origen):**

  Todo el tráfico de una IP de origen se envía a la misma interfaz.

- **Peso (basado en el peso):**

  Las interfaces con mayores pesos tienen mayor prioridad y obtienen más tráfico.

- **Spilover (basado en el uso):**

  Todo el tráfico se envía a la primera interfaz de la lista. Cuando el ancho de banda en esa interfaz excede el límite de desbordamiento, se envía tráfico nuevo a la siguiente interfaz.

- **IP de origen-destino (source-dest-ip-based):**

  Equilibrio de carga IP de origen y destino. Todo el tráfico de una IP de origen a una IP de destino se envía a La misma interfaz.

- **Volumen (basado en el volumen medido):**

  Balanceo de carga basado en volumen. Las sesiones están equilibradas en función del volumen de tráfico (en bytes[22]). Se envía más tráfico a las interfaces con relaciones de volumen más altas.

- **Por detección SLA (Acuerdo de nivel de servicio):**

  SLA de rendimiento, enviando periódicamente señales de sondeo a través de cada enlace de miembro a un servidor destino que actúa como una referencia para medir la latencia o degradación del enlace, a través de esta medición el algoritmo decidirá a que enlace enviar el tráfico de red

[22] **Bytes:** Unidad de medida de la información por ocho bits.

2.2.2.2. Performance SLA.

La calidad del servicio para el tráfico asociado de un SLA de rendimiento perteneciente a un enlace miembro SD-WAN, deberá cumplir el objetivo sobre los otros enlaces participantes. Puede configurar la latencia, la fluctuación de fase y el paquete umbrales de pérdida para satisfacer sus necesidades y crear SLA granulares para ajustar la SD-WAN para aplicaciones específicas. Los valores configurados, se usan solo cuando una regla hace referencia a ellos. Puedes crear múltiples SLA Target por rendimiento. Por ejemplo, está ubicado en una sucursal y utiliza algunas aplicaciones diferentes que se ejecutan en misma sede del servidor. Puede crear un SLA de rendimiento que realice la comprobación de estado en ese servidor, pero luego tienen diferentes objetivos de SLA para las diferentes aplicaciones. Podrías hacer las reglas para algunas aplicaciones básicas, pero más estrictas para otras. Sin embargo, si las aplicaciones se ejecutan en diferentes servidores, entonces querrá crear diferentes SLA de rendimiento para cada aplicación en para que la comprobación de estado vaya contra el servidor de la aplicación específica. Y cada actuación SLA requeriría solo un objetivo SLA para esa aplicación. Se utilizan tres criterios diferentes para esta medición, latencia, fluctuación de fase y porcentaje de pérdida de paquetes. Son estos valores los que se usan según los criterios de SLA dentro de las reglas que se usan para enrutar el tráfico basado en la calidad del enlace de cada miembro. La pérdida de paquetes, la latencia y el jitter que se muestran se basan en las respuestas (promediadas durante un breve período de tiempo), del servidor que está utilizando el rendimiento SLA. Si ese servidor deja de estar disponible, luego cambiará al segundo servidor. Se quedará con ese segundo servidor hasta que no esté disponible, momento en el que volverá al primer servidor (Fortinet INC, 2019, pág. 31).

Las reglas SD-WAN le permiten especificar qué tráfico desea enrutar a través de qué interfaz. Puedes configurar las reglas SD-WAN para elegir las interfaces de salida basadas en diferentes estrategias. Las reglas se evalúan en de la misma manera que las políticas de firewall: de arriba a abajo, utilizando la primera coincidencia. Puedes usar lo siguiente parámetros para que coincida con el tráfico:

- Dirección IP origen
- Dirección IP de destino
- Número de puerto de destino
- Aplicación de firewall como destino
- Tipo de servicio (ToS)

2.2.2.3. Autodiscovery Virutal Private Network (ADVPN).

ADVPN es utilizado en topologías de punto a multipunto se denomina hub and spoke[23], como su nombre lo describe, todas las sucursales se conectan a través de una central. Una ventaja de usar esta topología es que puede administrar fácilmente la configuración de VPN[24] y las políticas de firewall de forma centralizada, garantizando la seguridad en los enlaces permitiendo encriptar la información y que pueda ser entregada de forma segura y confiable mediante los protocolos de IKE[25] e IPsec[26]. Es una alternativa eficiente y segura es IPsec Auto-Discovery VPN (ADVPN), que permite una cantidad mínima de configuración por sitio, pero aún permite conexiones IPsec directas entre cada

[23] **Hub and Spoke:** Es un sistema de red que tiene una estación central conectado a varios hosts.
[24] **VPN:** Red Privada Virtual
[25] **IKE:** Internet Key Exchange, es un intercambio de llave secreta por internet
[26] **Ipsec:** Protocolo de Seguridad de Internet.

sitio. RFC[27] 7018 describe esencialmente este problema, junto con algunos requisitos para las soluciones candidatas, siendo esta solución una buena opción para la habilitación en una red corporativa. Una red ADVPN admite arquitecturas de concentrador único o múltiple NAT[28], requiere el uso de un protocolo de enrutamiento para su correcto funcionamiento. Actualmente, es compatible con los protocolos de enrutamiento BGP y OSPF[29]. A través de la solución de ADVPN mejora la administración de las VPNs de manera eficiente y centralizada. (Fortinet INC, 2019, pág. 180).

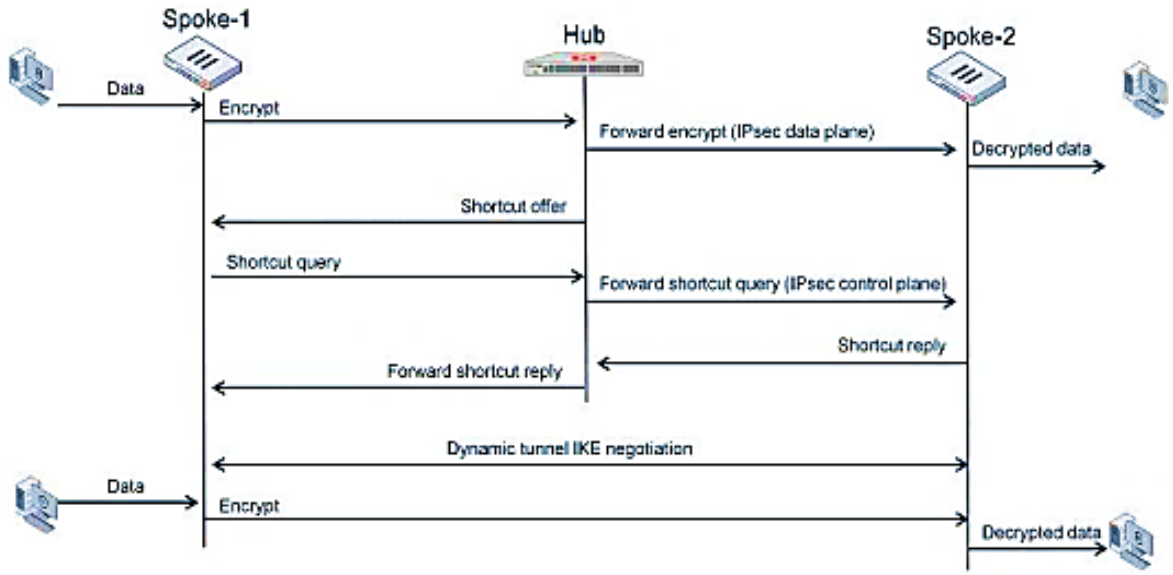


Figura 6. Flujograma de comunicación de una red ADVPN

Fuente: (Fortinet INC, 2020)

[27] **RFC:** Son un conjunto de documentos que sirven de referencia para la comunidad de internet.
[28] **NAT:** Network Address Translation, permite traducir direcciones privadas hacia la Internet.
[29] **OSPF:** Protocolo de enrutamiento por sus siglas Open Shortest Path First.

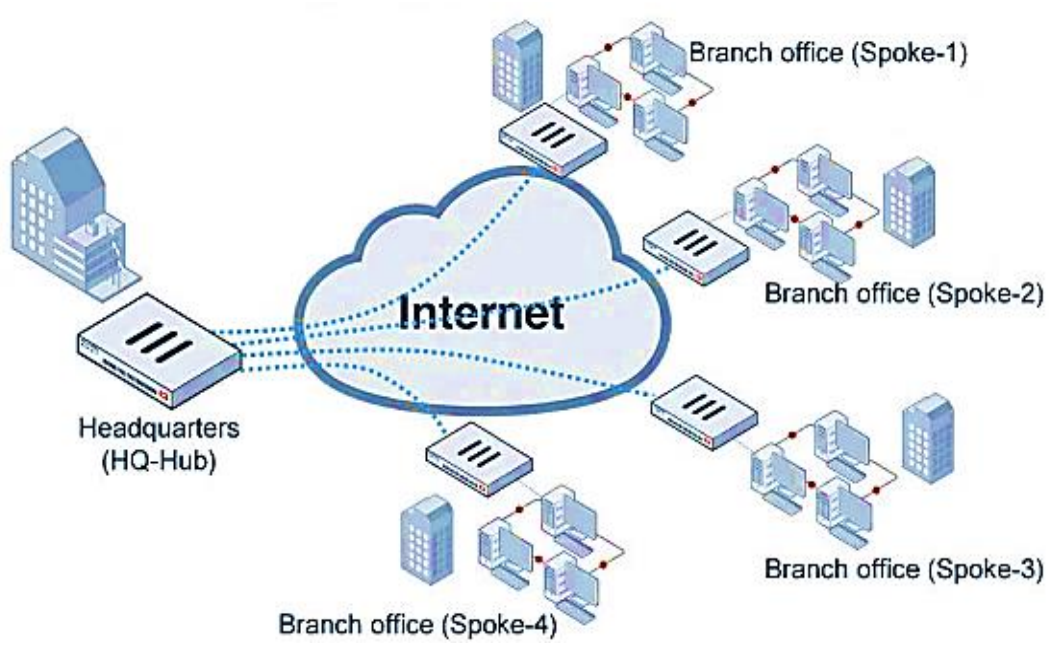


Figura 7. Topología Hub and Spoke

Fuente: (Fortinet INC, 2020)

2.2.2.4. Internet Protocol Security (IPsec).

Es una extensión del protocolo IP que brinda seguridad a IP y a los protocolos de capa superior. Fue desarrollado para el nuevo estándar de IP versión 6 (IPv6) y luego adaptado para implementarlo en la versión 4 (IPv4). IPSec utiliza dos protocolos diferentes para asegurar la autenticidad, integridad y confidencialidad, estos son el protocolo de Autenticación de Encabezado AH (Authentication Header) y el protocolo de Encapsulado de Seguridad de Datos o ESP (Encapsulated Security Payload). IPSec puede proteger todo el datagrama IP o solamente los protocolos de capa superior mediante los modos túnel y transporte. En el primer caso el datagrama IP es encapsulado en forma completa en otro. En el modo transporte solo los datos del datagrama IP original es procesada por IPSec, insertando el encabezado AH o ESP entre el encabezado IP y los datos. Para asegurar la

integridad del datagrama IP, IPSec utiliza HMAC14 (Hash Message Authentication Code) o Código de autenticación de mensajes basados en hash[30], mediante algoritmos como MD5 y SHA. Lo calcula basado en una clave secreta y en el contenido del datagrama.

Lo calcula basado en una clave secreta y en el contenido del datagrama. IPSec utiliza algoritmos de encriptación simétricos estándar de elevada fortaleza como 3DES[31], AES[32] o Blowfish [33]para asegurar la confidencialidad del tráfico transportado. IPSec protege la comunicación respecto de ataques de denegación de servicio o ataques de repetición, mediante el mecanismo de ventana deslizante. Los números de secuencia de los paquetes deben estar dentro del rango aceptado por la ventana, sino son descartados.

2.2.2.5. Ventajas de usar ADVPN.

El tesista (Vásquez, 2012), elaboró las siguientes ventajas de una Red Privada Virtual (p.8):

- Costo de implementación reducido: Cuestan considerablemente menos que las soluciones tradicionales, que están basadas en líneas arrendadas sobre MPLS. Esto porque los VPN eliminan la necesidad de conexiones de larga distancia reemplazándolas con conexiones locales a una red transportista, ISP o El Punto de Presencia de ISP (POP).
- Costos de personal y administración reducidos: Mediante la reducción de los costos de telecomunicación de larga distancia, los VPN bajan considerablemente los costos de las operaciones de red basadas en WAN. En

[30] **Hash:** Es un algoritmo matemático para el intercambio de llaves públicas por internet.
[31] **3DES:** Triple Data Encryption Algorithm, es una clave simétrica de cifrado por bloques.
[32] **AES:** Avanced Encryption Standard, es un esquema de cifrado avanzado por bloques
[33] **Blowfish:** Es un codificador de bloques simétricos, es una técnica de criptografía de red.

adición, una organización puede reducir el costo total de la red si el equipo WAN usado en el VPN es administrado por el ISP.

- Conectividad: Los VPN usan la Internet para interconectividad entre partes lejanas de una intranet. Debido a que la Internet es globalmente accesible, incluso las oficinas más lejanas, usuarios, y usuarios de móviles (como los vendedores) pueden fácilmente conectarse a la intranet corporativa.
- Seguridad de transacción: Ya que los VPN usan la tecnología de túnel para transmitir datos a través de redes públicas "inseguras", las transacciones de información son seguras hasta un alcance. Además de la tecnología de túnel, los VPN usan medidas de seguridad extensivas, como la codificación, autenticación y autorización para salvaguardar la seguridad, confidencialidad e integridad de la información transmitida.

2.2.2.6. Protocolo de Enrutamiento de Border Gateway (BGP).

Es el sistema que utilizan los grandes nodos de Internet para comunicarse entre ellos y transferir una gran cantidad de información entre dos puntos de la Red. Su misión es encontrar el camino más eficiente entre los nodos para propiciar una correcta circulación de la información en Internet a través de costos. Los grandes nodos que permiten que la información fluya por Internet suelen utilizar routers[34] que funcionan bajo el protocolo BGP. Cuando una persona envía un correo electrónico desde Madrid a, por ejemplo, Montevideo, los sistemas de su proveedor de Internet buscarán el camino más rápido para

[34] **Routers:** En un equipo ruteador o encaminador que sirve para interconectar redes.

que dicho e-mail llegue a su destinatario, Opera intercambiando información de rutas y garantiza un camino libre de loops.

El protocolo BGP[35] usa TCP[36] como protocolo de transporte (puerto 179), se establece entre un par de routers (neighbors o peers) una sesión TCP abierta, mediante la cual intercambian información de ruteo BGP, Los peers [37]BGP no necesitan estar directamente conectados. Como trabaja BGP:Aprender una Ruta: significa que voy a incorporar en mi tabla de BGP alguna ruta que me están enseñando (Cisco System, 2018, pág. 1).

Cada AS tiene un identificador: ASN (Autonomous System Number). ASN: 16 o 32 bits.

Número de AS/bloque	Asignación
0 y 65535	Reservados
entre 1 y 64495	Internet Pública
entre 64496 y 64511	Documentación para ASN 16 bits – RFC 5737
entre 64512 y 65534	Uso sólo privado
entre 65536 y 65551	Documentación para ASN 32 bits – RFC 5398
entre 65552 y 4294967295	Internet Pública

Figura 8. Asignación de ASN por IANA

Fuente: (LACNIC, 2018)

[35] **BGP:** Border Gateway Protocol, es un protocolo de enrutamiento dinámico.
[36] **TCP:** Protocolo de control de transmisión
[37] **Peers:** Vecino que establece una adyacencia en un enrutamiento de redes

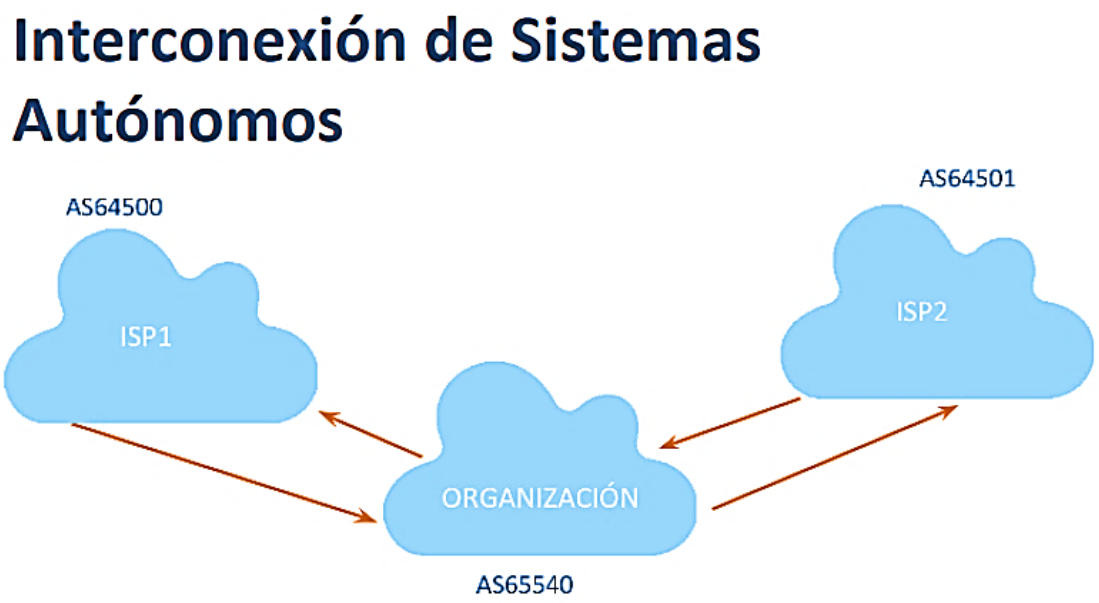


Figura 9. Arquitectura eBGP

Fuente: (LACNIC, 2018)

Para, (Lacnic INC, 2018), menciona los siguientes contenidos para definir la comunicación del protocolo de enrutamiento de BGP (p.14):

- Aprender una Ruta: significa que voy a incorporar en mi tabla de BGP alguna ruta que me están enseñando.
- Anunciar una ruta: significa que le voy a decir a alguien que tengo una ruta para llegar a determinado destino, y que esa ruta está en la tabla de ruteo.
- Sistema Autónomo: Grupo de redes IP que comparten una política de ruteo propia e independiente.
- Anunciar una ruta: significa que le voy a decir a alguien que tengo una ruta para llegar a determinado destino, y que esa ruta está en la tabla de ruteo.
- Sistema Autónomo: Grupo de redes IP que comparten una política de ruteo propia e independiente.

- En conexión: Uno de los extremos intenta una conexión TCP.
- Activo: Cuando uno de los extremos no puede establecer conexión y lo reintenta periódicamente.
- Establecido: Se aceptan las identificaciones. De aquí en adelante, la sesión se considera completamente activa.

2.2.2.7. Traffic Shaping.

El traffic shaping intenta normalizar los picos y las ráfagas de tráfico para priorizar ciertos flujos sobre otros. Proporciona calidad de servicio al aplicar límites de ancho de banda y priorización. Usando el tráfico dando forma, puede ajustar cómo su CPE [38]asigna recursos a diferentes tipos de tráfico, para mejorar la rendimiento y estabilidad de las aplicaciones de red sensibles a la latencia o al ancho de banda.

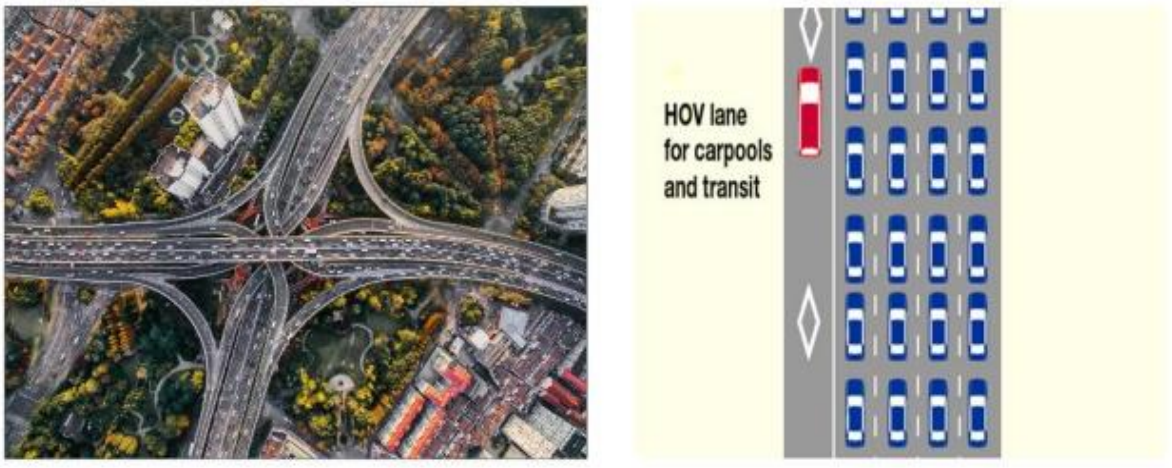


Figura 10. Esquema de priorización de tráfico

Fuente: (Fortinet INC, 2020)

[38] **CPE:** Customer Premises Equipment o en sus siglas en español (Equipo Local del Cliente).

Debido a que el ancho de banda es finito y a que algunos tipos de tráfico son lentos, fluctúan o son sensibles a la pérdida de paquetes, el ancho de banda intensivo o la operación crítica, QoS[39] puede ser una herramienta útil para optimizar el rendimiento de diversas aplicaciones en su red. Descubrir las necesidades y la importancia relativa de cada tipo de tráfico en su red lo ayudará a diseñar un enfoque general apropiado, incluyendo cómo configurará cada técnica de componente de QoS disponible. La vigilancia del tráfico es descartar paquetes que no se ajustan a las limitaciones de ancho de banda. El modelado del tráfico consiste en una mezcla de vigilancia del tráfico para hacer cumplir los límites de ancho de banda y la cola de prioridad ajuste para ayudar a los paquetes a alcanzar la tasa garantizada. La puesta en cola garantiza que los paquetes se transmitan en el orden de la cola de prioridad asignada para dicha interfaz física.

Al configurar el modelado de tráfico para su red, existen tres métodos diferentes para controlar el flujo de tráfico de red para garantizar que pase el tráfico deseado y al mismo tiempo limitar el ancho de banda para los menos importantes o tráfico que consume ancho de banda. Hay tres métodos:

- La configuración de políticas le permite definir el ancho de banda máximo y el ancho de banda garantizado establecido para una política de seguridad.
- La configuración por IP le permite definir el control del tráfico en un nivel más granular.
- La configuración basada en la interfaz va más allá, permitiendo controles de tráfico basados en el porcentaje de la interfaz

[39] **QoS:** Calidad de Servicio

La opción del máximo ancho de banda establecerá la mayor cantidad de tráfico permitido utilizando una política donde este modelador es habilitado Si el tráfico supera este límite, comenzará a descartar paquetes. La opción de ancho de banda garantizado garantiza que haya un ancho de banda reservado consistente disponible para el tráfico pasando por la política. Debería ser significativamente menor que la capacidad de ancho de banda de la interfaz. Si no es así causará latencia no deseada para otro tráfico que pase por esa política de modelado. En la lista desplegable Prioridad de tráfico, puede seleccionar Alto, Medio o Bajo. Cuando la opción por política está deshabilitada (el valor predeterminado es deshabilitar), aplica reglas de configuración a todas las políticas que usan la prioridad de tráfico. Si la opción por política está habilitada, aplica reglas de configuración a cada política individualmente. En el ejemplo que se muestra en esta diapositiva, se asignan 30 Mbps[40] de ancho de banda máximo y 10 Mbps de ancho de banda garantizado, Por lo tanto, el tráfico que pasa por esta política tendrá garantizados 10 Mbps de ancho de banda en cualquier momento punto en el tiempo (Fortinet INC, 2019, pág. 95).

2.3. Marco metodológico

2.3.1. Metodología PPDIOO.

Para el desarrollo del marco metodológico de la presente tesis se ha seleccionado la metodología PPDIOO que define las actividades bajo un ciclo de vida que permitirá cumplir los objetivos trazados, logrando agilizar, optimizar y operar de forma exitosa la administración de red para la implementación de una nueva estructura de comunicaciones.

[40] **Mbps:** Megabit por segundo, es una unidad de transmisión de datos equivalente a 1.000.000 bits.

Las siglas del modelo PPDIOO obedece a las diferentes etapas en quede dividir el ciclo de vida de una red:

- Preparar: La identificación de la tecnología que soportará la arquitectura.
- Panificar: Identificar lo que la red necesita.
- Diseñar: Elección de la solución óptima.
- Implementar: Crear la red
- Operar: Probar y poner en funcionamiento
- Optimizar: Mejorar la red y arreglar problemas.

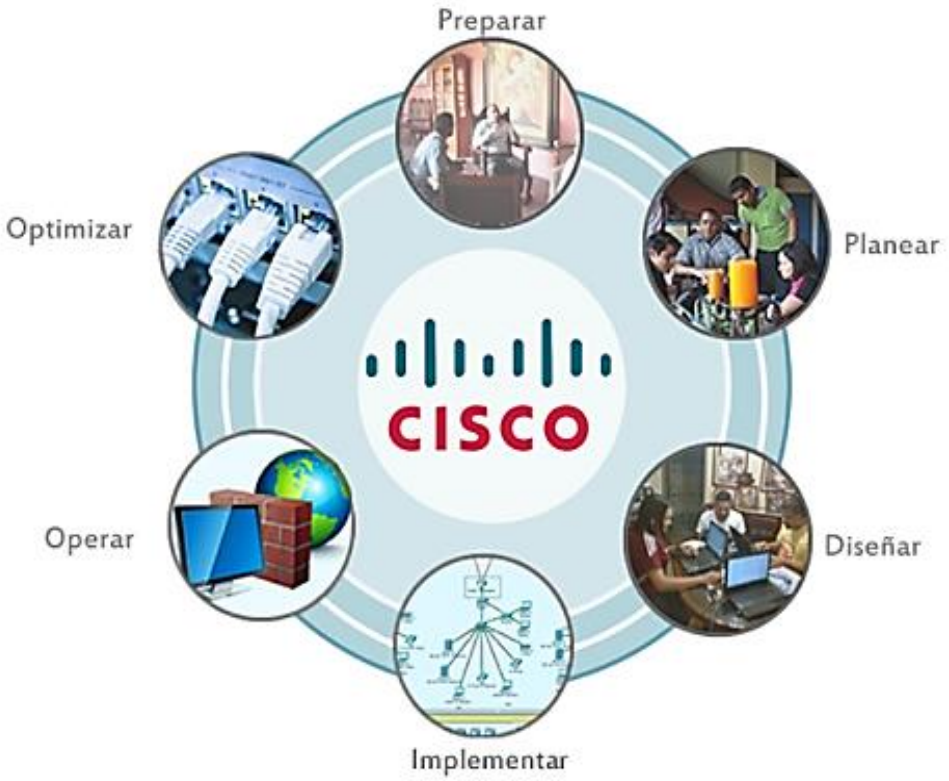


Figura 11. Ciclo de Vida de PPDIOO

Fuente: (Cisco System, 2018)

2.3.1.1. Beneficios de PPDIOO.

En resumen, (Erazo, 2016) “Menciona los siguientes beneficios de PPDIOO” (p.46):

- Disminución de costo de propiedad
- Aumento de disponibilidad de la red
- Agilidad de los negocios
- Mayor velocidad de acceso a aplicaciones y servicios
- Optimización en el desempeño de la red

2.3.1.2. Fases del ciclo de vida PPDIOO.

El objetivo de este proceso es racionalizar y simplificar el trabajo a realizar, y de alguna manera automatizar parte del proceso realizado. Esto es secuencial porque separa claramente diferentes etapas del ciclo de vida. Debido a que continuamente retroalimenta, es iterativo. Para implementar esta metodología, es necesario registrar todo lo realizado en cada etapa (Erazo, 2016, pág. 2).

2.3.1.2.1. Preparación.

En esta fase, creará un caso de negocio para establecer la justificación financiera para una estrategia de red. Lo cual, Satisfaga las necesidades comerciales prediciendo cuidadosamente lo esperado a futuro, lo que permitirá desarrollar una arquitectura con todos los requisitos para el buen funcionamiento de la solución, definidos en:

- **Servicios y aplicaciones de red:** Actualmente se deben verificar las aplicaciones y servicios que soportan la red, así como las aplicaciones y servicios a implementar.
- **Objetivos Organizacionales:** Se propondrán metas más específicas, como la reducción de costos, la incorporación de productos basados en tecnología de punta y la provisión de nuevos servicios para los usuarios finales.
- **Restricciones organizacionales:** Estos límites suelen plantearse por cuestiones de presupuesto y tiempo, pero pueden platearse por políticas internas o externas (Gobierno o leyes).
- **Objetivos técnicos:** Deben estar alineados con los objetivos organizacionales, pero desde la perspectiva técnica. Por ejemplo: proporcionar escalabilidad de la red, reducir las fallas de los equipos, simplificar la administración de la red, modernizar la infraestructura de red, etc.
- **Caso de negocio:** Se mostrará la viabilidad del proyecto.

2.3.1.2.2. Planificación.

En esta fase, se determinarán todos los requisitos de la red. Se analizó la nueva tecnología y se determinará la forma que se desarrollará el uso de la red para la empresa. También hay que tener en cuenta que puede iniciarse desde cero o desde la red de producción.

Asimismo, es importante determinar todo lo que afectará a la red. Estos factores pueden ser muchos y dependen de la solución o arquitectura propuesta:

- Conexiones simultaneas de usuarios
- Aplicaciones que se utilizaran en la red
- Escalabilidad
- Adaptabilidad
- Medio físico
- Servicio de red y tipo de tráfico
- Disponibilidad y redundancia de red
- Coste de los recursos y duración de estos
- Requisitos de seguridad

2.3.1.2.3. Diseñar.

En esta fase, se ejecutará la planificación lógica y física de la red. Hay que decidir cuál será la mejor distribución en la red. Uno de los primeros pasos es diseñar la red en base a la información obtenida en la fase anterior.

El plan de proyecto se ha actualizado para proporcionar información más detallada, que se utilizará en la implementación:

- Arquitectura bajo nivel
- Plan de Migración
- Pruebas de verificación del diseño

2.3.1.2.4. Implementación.

En esta fase, se realizará la instalación de los equipos con sus configuraciones. El nivel de documentación obtenido debe proporcionar información detallada para cada paso a

realizar, así como el tiempo de ejecución, plan de trabajo y un plan de contingencia en caso se requiera ejecutar rollback[41] de las configuraciones en caso ocurra una falla en la implementación. Es fundamental para lograr este objetivo ejecutar un piloto de pruebas en un entorno virtualizado (preproducción). Acá se entrega el siguiente entregable: Plan de trabajo para la implementación de red

2.3.1.2.5. Operación.

En esta fase, se realizarán las tareas de monitoreo y administración de la red. Los posibles problemas de rendimiento generalmente se identifican aquí, las incidencias se deberán corregir y documentar. Esta fase suele ser el último paso para finalizar el diseño. El principal objetivo es el mantener un estado de salud óptimo de la red al fin de brindar un mejor servicio, reduciendo las interrupciones y proveer mayor disponibilidad, fiabilidad y seguridad a la red. Al mismo tiempo, debe ayudar a reducir costos y brindar medidas preventivas y correctivas inmediatas, siempre y cuando no se presenten al usuario final. Esta fase requerirá de la implementación de herramientas de monitoreo de red, pueden ser las mismas que se utilizarán en la fase de Planeación. En cuanto a los documentos entregables en esta fase existen:

- recreación de problemas.

2.3.1.2.6. Optimización.

En esta fase se ejecutarán acciones proactivas que resuelvan cuestiones identificadas en la fase de Operación, de presentarse demasiados problemas podría requerir una

[41] **Rollback**: Restablecer o reversión del servicio.

modificación del diseño realizado e incluso iniciar las fases anteriores. El objetivo principal es mejorar el desempeño de la red sin interrumpir la operación y adaptándose a las necesidades del día a día. En lo que respecta a documentos entregables de esta fase se tiene:

- Pruebas de Aceptación del Software.

2.3.2. Matriz RACI

De acuerdo (Pursell, Shelley, 2020), “RACI es un diseño gráfico que permite gestionar la asignación de roles y responsabilidades para monitorear las tareas que componen un proyecto de equipo. Promueve la comunicación entre todos y agiliza el proceso de toma de decisiones”. La razón de esto se encontrará en la clasificación de los participantes del equipo de trabajo. Se divide en cuatro categorías (p.1).

2.3.2.1. Responsables.

La primera categoría o rol en la matriz RACI es la de los responsables, quienes se encargarán de realizar las tareas pendientes en un proyecto.

Pueden participar en diferentes actividades según la situación, como redacción de contenidos, creación de imágenes o material audiovisual. Cuando necesita elegir múltiples opciones de ejecución los responsables son los encargados de dicha actividad.

2.3.2.2. Autoridad.

La siguiente categoría encontrarán a los responsables de la Administración. Especificarán la categoría de cada persona en el proyecto. Además, también se encargan de registrar y responder al completar la tarea. De esta manera, conocen el avance del proyecto

desde las tareas más simples hasta las más complejas. Ellos serán los que sepan cuándo completar cada tarea a completar en todo el proyecto.

2.3.2.3. Consultados.

En la tercera categoría, encontrará a los Consultores. Ellos conocen las características de cada tarea asignada. Debido a que conocen esta información, una vez que el responsable la ejecute, comentará cada actividad pendiente.

Si el responsable tiene dudas sobre un aspecto particular de la tarea que le corresponde, puede acudir a un consultor. El responsable es propietario de esta información.

2.3.2.4. Informados.

La última categoría son los Informantes. Comprenderán el progreso del proyecto, no solo al completar tareas como sucede en el caso de la Autoridad. Cuando el responsable de tareas toma una decisión, el reportero será la persona a quien se le dijo la elección. Lo mismo ocurrirá si hay algún inconveniente o problema durante la tarea.

Figura 12. Modelo de Matriz RACI

Fuente: (Jorge Saiz, 2019)

CAPÍTULO III

Planteamiento de la Metodología Protocolo Secure SD-WAN

3.1. Metodología de la Investigación

En base a lo expresado en el Capítulo I “Antecedentes del Problema”, se utilizará la Metodología de investigación aplicada, la cual se enfoca en resolver la situación actual o problemas concretos e identificables de la empresa Cencosud S.A.

3.1.1. Alcance de la investigación

El alcance de investigación es del Tipo Exploratoria, que permitirá tener un conocimiento general del tema para desarrollar una solución en el futuro. Por lo tanto, se tendrá una idea aproximada y previa de algo sobre lo que aún no existen estudios previos, y sirven como información general para estudios tecnológicos.

3.1.2. Diseño de la Investigación

El diseño de investigación es del tipo No Experimental, se refiere al plan o estrategia concebida que analizará los resultados de la solución. Por lo tanto, tiene objetivo de observar lo que realmente sucede sin manipular las variables.

3.2. Metodología de Trabajo

En base a lo desarrollado en el Capítulo II donde se indica el "Marco Metodológico" a utilizar, la metodología PPDIOO es un modelo que optimiza la implementación de cambio en una red existente, su objetivo primordial es reducir el costo de inversión, garantizar la administración total de red y brindar el aumento de disponibilidad en la infraestructura de Telecomunicaciones para finalmente proveer un diseño acuerdo al requerimiento del cliente. Lo que mejorará lo precisado en el Capítulo I "Antecedentes del Problema".

Consta de 06 etapas dentro del ciclo de vida que brinda un marco de referencia que permita aplicarlos al área de Telecomunicaciones de la empresa Cencosud S.A. De este modo, que cumpla los objetivos técnicos como los procesos del negocio.

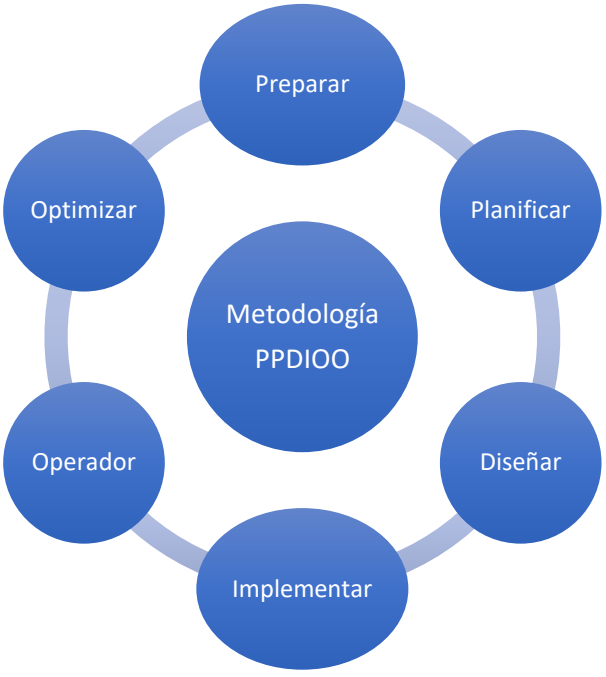


Figura 13. Esquema de PPDIOO

Fuente: Elaboración Propia

En el siguiente diseño de se mostrará las fases de la metodología de PPDIOO empleado para el diseño de Protocolo de Secure SD-WAN y los beneficios que brinda desarrollar la metodología para la implementación de la solución propuesta.

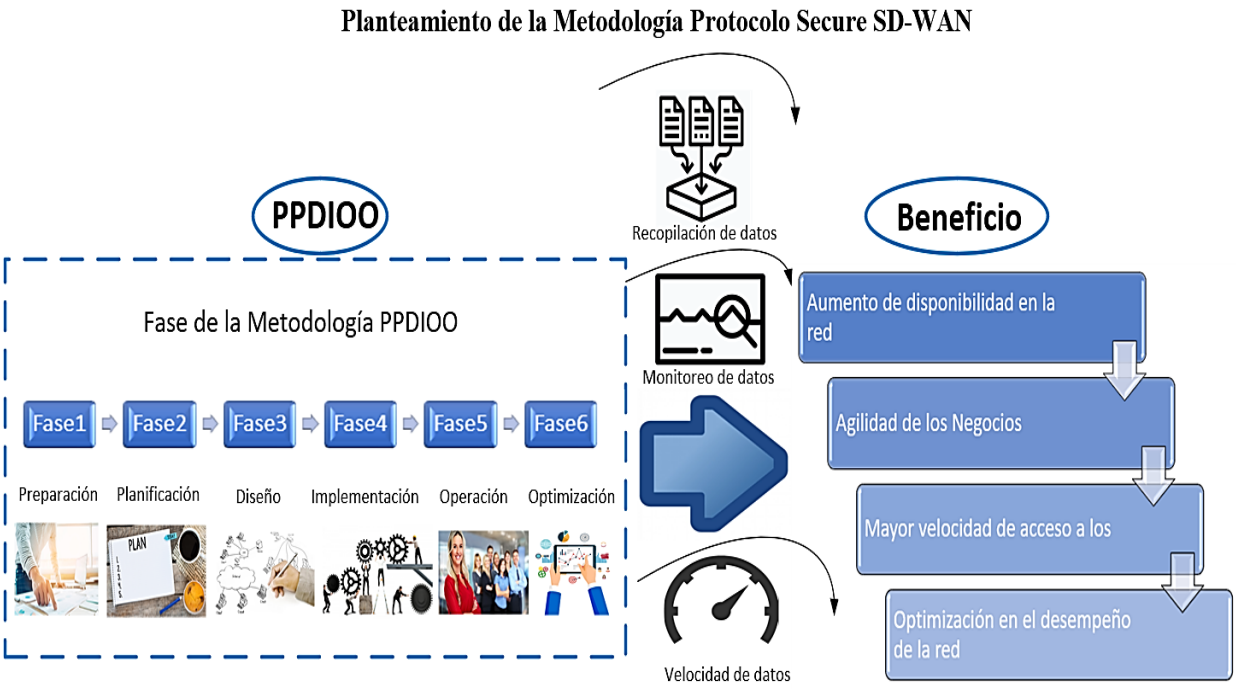


Figura 14. Pictografía de la Metodología PPDIOO

Fuente: Elaboración Propia

3.2.1. Etapa 1 Preparación

En la actualidad, la empresa Cencosud S.A. carece de una red altamente disponible, es decir, qué, ante cualquier incidencia de congestionamiento de tráfico de la red o avería de fibra óptica, la compañía sufriría graves consecuencias en la paralización del negocio generando pérdidas tangibles. Es por ello qué presentará el proyecto de tesis donde se planteará una nueva alternativa de diseño tecnológico en el campo moderno de las comunicaciones informáticas. Es por ello qué, se presentará el protocolo Secure SD-WAN, el cual brindará diversos beneficios a la infraestructura de red del cliente, aplicando técnicas de algoritmos inteligentes que ofrecerá una red altamente disponible, con tiempos predecibles ante cualquier avería de enlaces, garantizando la continuidad del negocio, reforzando así la red con valores de optimización de tráfico y niveles de seguridad. En tal sentido, se justifica en el campo económico la inversión de la presente solución, otorgando una reducción de costos ante las pérdidas que sufriría la compañía ante alguna falla o avería en la red de producción.

Para tal efecto, se plasmará la siguiente figura donde, se presentará de forma visual los problemas identificados en la red de Cencosud S.A, expuesto En el Capítulo I “Antecedentes del Problema”. Por otra parte, se detallarán los beneficios que brindaría la implementación de la solución propuesta en el negocio de la empresa.

Figura 15. Los problemas que atraviesa Cencosud S.A.

Fuente: Elaboración Propia

Figura 16. Beneficios que ofrece SD-WAN

Fuente: Elaboración Propia

En la siguiente figura, se mostrarán los requerimientos necesarios para el desarrollo del proyecto, así el cliente podrá evaluar y finalizar con la aprobación para la viabilidad del caso negocio, teniendo como único objetivo de satisfacer las necesidades del cliente.

Figura 17. Requerimientos de Preparación

Fuente: (Elaboración Propia, 2020)

3.2.2. Etapa 2 Planificación

En esta etapa, se llevará a cabo la planificación de las actividades en la Tabla 1, la asignación de roles y responsabilidades. Asimismo, se expondrá la recolección de información de los recursos de red de la empresa Cencosud S.A, que serán de utilidad para el desarrollo del diseño de red. Por último, se elaborará el cronograma de actividades.

Tabla 1

Actividades que cubrirán el ciclo de vida de la Metodología PPDIOO

Ítem	Etapa	Actividades	Resultado
1	Preparación	Se presentará el caso negocio	Inversión del proyecto
2	Planificación	Se elaborará el cronograma de actividades	Roles y Responsabilidades
3	Diseño	Se diseñará la arquitectura propuesta	Diseño de alto nivel
4	Implementación	Se ejecutará la simulación y configuraciones de la solución	Desarrollo de la solución
5	Operación	Se monitoreará y se validará el estado de los servicios	Puesta en marcha
6	Optimización	Se realizará los afinamientos de configuraciones	Red óptima

Nota: Se muestra las 6 etapas del ciclo PPDIOO, Autoría propia.

3.2.2.1. Identificación de los Recursos de Red.

En la Tabla 2, se utilizará el objetivo específico 1, donde se recopilará los datos de carga como los recursos de red y las herramientas de uso de la empresa con el fin de obtener la información para el desarrollo la propuesta técnica del equipamiento para la solución SD-WAN que será presentados en el Capítulo IV “Desarrollo de la Metodología en la etapa de Preparación”.

Tabla 2

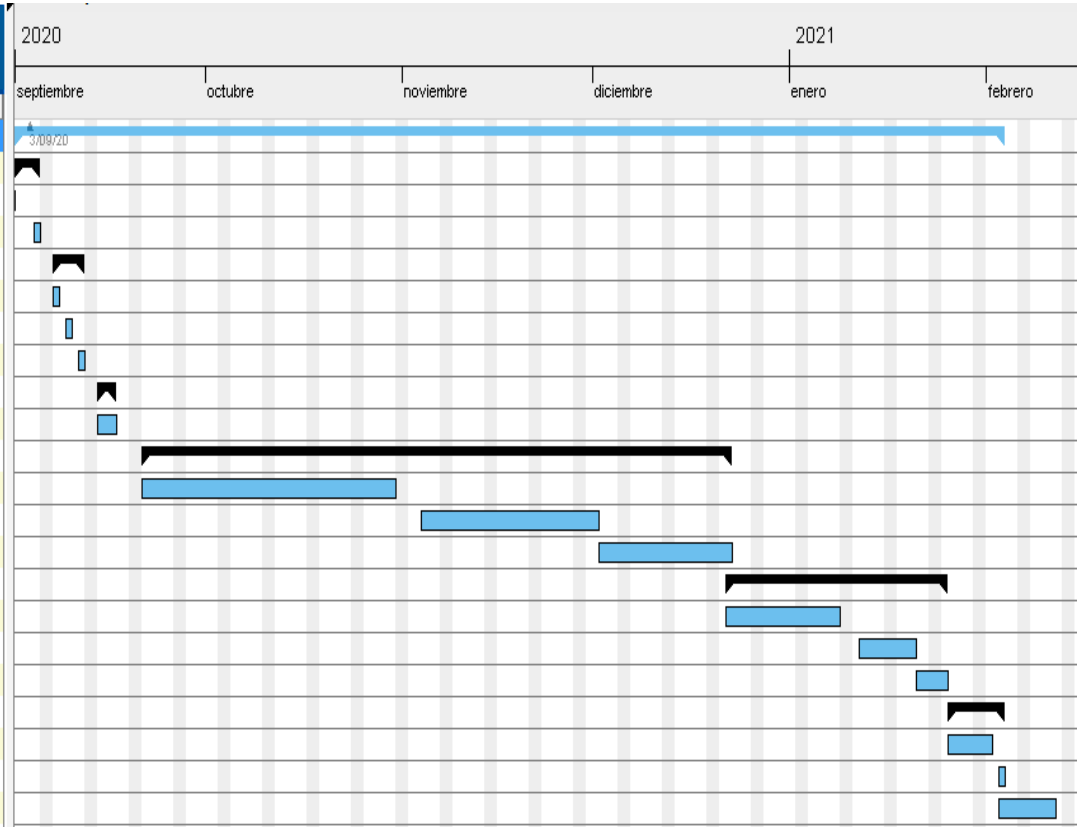
Información de los recursos de red de Cencosud S.A.

Ítem	Recursos	Contenido
1	Sistemas Informáticos	Sistema de Caja
		Sistema de Facturación Electrónica
		Sistema de Logística
		Intranet
2	Sesiones concurrentes	15,000
3	Cantidad de usuarios	2, 700
4	Uso de ancho de banda	Central: 150 Mbps
		Tiendas: 4 Mbps
5	Número de sedes en Lima	89 tiendas
6	Datos de Carga	Central: 160 Mbps
		Tiendas: 7 Mbps

Nota: Se toma la recopilación de la información de los recursos de red. Autoría propia.

3.2.2.2. Cronograma de Actividades.

Nombre	Duración	Fecha de inicio	Fecha de fin
Inicio del Proyecto	113	31/08/20	3/02/21
Etapa I-Preparación	5	31/08/20	4/09/20
Presentación del Caso Negocio	1	31/08/20	31/08/20
Aprobación del Proyecto	1	4/09/20	4/09/20
Etapa II-Planificación	5	7/09/20	11/09/20
Elaboración de Tabla I - Actividades	1	7/09/20	7/09/20
Asignación de Roles y Responsabilidades	1	9/09/20	9/09/20
Identificación de los Recursos de Red	1	11/09/20	11/09/20
Etapa II-Diseño	3	14/09/20	16/09/20
Elaboración del Diseño Propuesto	3	14/09/20	16/09/20
Etapa IV-Implementación	67	21/09/20	22/12/20
Inicio de la simulación	30	21/09/20	30/10/20
Resultados de la simulación	20	4/11/20	1/12/20
Inicio de las configuraciones	15	2/12/20	22/12/20
Etapa V-Operación	25	22/12/20	25/01/21
Monitoreo de Red	14	22/12/20	8/01/21
Prueba y Muestreo	7	12/01/21	20/01/21
Instrumento de Medición	3	21/01/21	25/01/21
Optimización	7	26/01/21	3/02/21
Mejoramiento de los Resultados	5	26/01/21	1/02/21
Conclusiones	1	3/02/21	3/02/21
Fin del Proyecto	7	3/02/21	11/02/21



3.2.3. Etapa 3 Diseño

Para el planteamiento de la Etapa de Diseño, se elaboró la Tabla 3 donde, se especifica las tareas que se aplicarán para la entrega de la Arquitectura que entrará en remplazo de la arquitectura actual que contribuirá en el desarrollo del Capítulo IV "Desarrollo de la Metodología Protocolo Secure SD-WAN" para la etapa de diseño que brindará todas las especificaciones para la mejora tecnológica de la infraestructura de Telecomunicaciones de la empresa Cencosud S.A.

Tabla 3

Tareas de la Etapa de Diseño

Ítem	Tareas	Herramientas
1	Se presentará el diseño de la Arquitectura propuesta con las mejoras técnicas	Microsoft Visio
2	Se entregará la propuesta de equipamientos que participará en la solución de la empresa	Datasheet[42]
3	Se presentará el diseño de red que participará en la simulación de la red para las pruebas de Concepto	Microsoft Visio

Nota: Distribución de las tareas de la Etapa de Diseño. Autoría propia.

[42] **Datasheet:** Ficha técnicas de equipamientos.

3.2.4. Etapa 4 Implementación

En esta etapa, se implementará la solución en un ambiente virtual a través de la simulación de red, de acuerdo con la información recopilada y el diseño de red propuesto, para extraer los resultados en la fase de prueba. Para tal efecto, se construyó la Tabla 4 donde se identificará el Plan de trabajo y los procesos de implementación.

Tabla 4

Procesos de la Etapa de Implementación

Ítem	Tareas	Herramientas
1	Se realizará la simulación de red	GNS3[43], VMware[44]
2	Se entregará el checklist de configuraciones	Microsoft Excel
3	Actualización de la documentación y diseño de red en la finalización de la implementación	Microsoft VISIO
4	Comprobación de las configuraciones de la simulación	Microsoft Word

Nota: Distribución de las tareas de la Etapa de Implementación. Autoría propia.

3.2.5. Etapa 5 Operación

Durante el proceso de Operación, la red será monitoreada de forma continua para la resolución de algún incidente en la red que puedan afectar a los usuarios finales, se deberá mantener una gestión y monitoreo constante de la red de datos, a través de las herramientas CACTI y PRTG que cumplirá la función de recabar y notificará algún incidente por la

[43] **GNS3:** Herramienta de simulación de red.
[44] **VMware:** Herramienta de virtualización de sistemas de red

administración de alertas en tiempo real, a través de este proceso se podrá mapear el objetivo específico 2 y 3, donde se determinará como contribuye la capacidad de red para el uso de balanceo de carga y el seguimiento del monitoreo de los enlaces de SD-WAN.

Tabla 5

Procesos de la Etapa de Operación

Ítem	Tareas	Herramientas
1	Se establecerá procedimiento de monitoreo	Microsoft Visio
2	Se definirá el procedimiento de los registros de la Bitácora de hecho y relevantes	Microsoft Excel
3	Se definirá las actividades del mantenimiento preventivo	Microsoft Excel
4	Se elaborará el procedimiento de RMA[45]	Microsoft Visio

Nota: Distribución de las tareas de Monitoreo y Control. Autoría propia.

3.2.6. Etapa 6 Optimización

Para culminar con el proceso de PPDIOO, en esta etapa se corregirá los posibles problemas a presentarse en la red. Por consiguiente, se documentará y se efectuará la entrega de monitoreo diario para optimizar la red, mejorando así continuamente de la infraestructura de Telecomunicaciones de Cencosud S.A.

[45] **RMA:** Proceso de Autorización de devolución de mercancía.

CAPÍTULO IV

Desarrollo de la Metodología Protocolo Secure SD-WAN

Luego de lo desarrollado en el Capítulo III “Planteamiento de la Metodología”, se procederá en el presente Capítulo IV a desarrollar la Fase de Diseño del Protocolo Secure SD-WAN para la empresa Cencosud S.A. En base a las necesidades expuestas del negocio en que está enfocada el trabajo de tesis y proveer todos los recursos necesarios para la elaboración del desarrollo de la metodología.

4.1. Definición del caso Actual

De acuerdo con lo expuesto en el Capítulo I “Antecedentes de Problema”. Se resume la situación actual que presenta el área de Telecomunicaciones de la empresa Cencosud S.A. Desde la perspectiva técnica, la empresa tiene 89 tiendas en la provincia de Lima donde opera los enlaces de L2L desplegados sobre la red MPLS, logrando la intercomunicación entre las tiendas con el fin de intercambiar la comunicación de los sistemas informáticos con la Oficina Central, los enlaces están distribuidos con un ancho de banda de 150 Mbps en la Oficina Central y 4 Mbps en cada tienda remota.

En la medida que se tuvo un crecimiento exponencial en la empresa, la Gerencia de Networking comenzó a percibir un incremento de tráfico en los enlaces de L2L, ocasionando cuellos de botella, lo cual genera retrasos en los accesos a los sistemas informáticos notando la molestia de los usuarios de la red y esto por el uso desmedido del ancho de banda en todas las tiendas. Ahora bien, a parte del problema del congestionamiento de red se suma también la falta de disponibilidad en la arquitectura de

red. Es decir, que si ocurre una avería de fibra óptica de alguno de los enlaces de L2L conllevaría a la pérdida de la comunicación entre las tiendas lo cual generaría un gran impacto negativo en la producción del negocio.

En las siguientes imágenes, se evidencia el congestionamiento de la red que sufre la empresa en los enlaces de transmisión de datos (L2L).

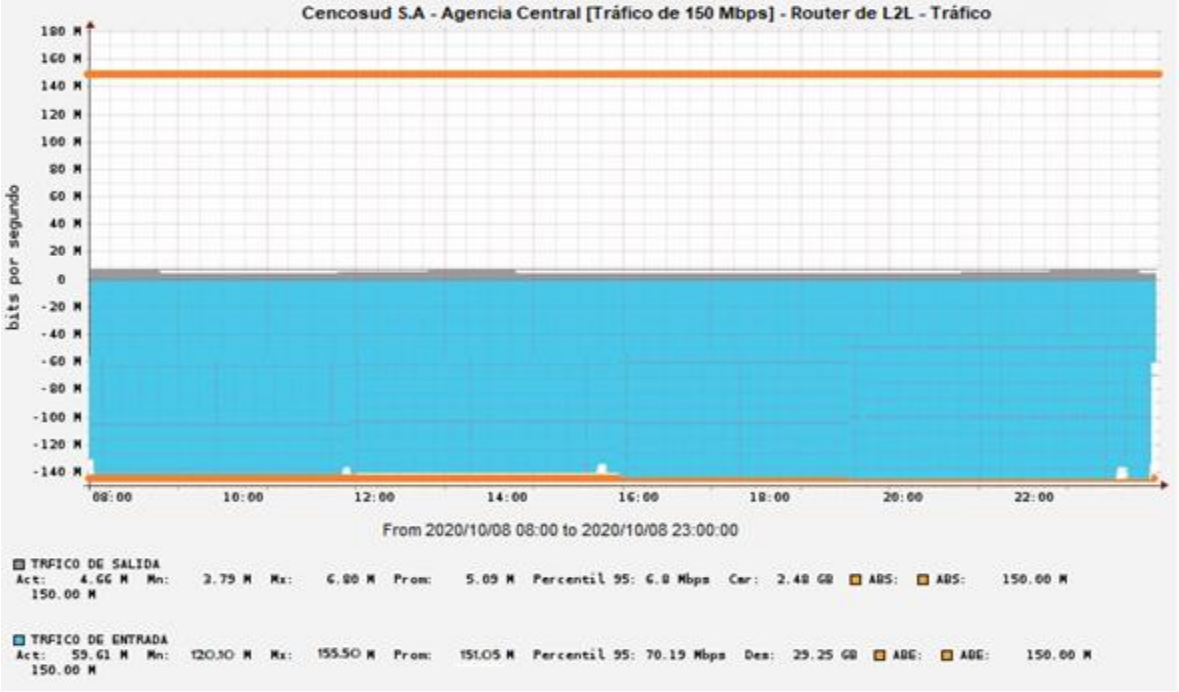


Figura 18. Tráfico de la Oficina Central

Fuente: (Elaboración Propia, 2020)

Para la evidencia de congestionamiento de red, se generó una estadística del consumo del tráfico de red de las tiendas de Cencosud S.A, a través de un reporte de los enlaces de L2L ejecutados en la herramienta Cacti Monitor de forma diaria. Al comparar estas evidencias como se visualiza en la imagen de la oficina central refleja el congestionamiento del tráfico de entrada (descarga) marcado en el historial de color celeste, sobrepasando el ancho de banda contratado de 150 Mbps configurado como indicador en la

gráfica con Línea naranja, el congestionamiento de los enlaces se registra en toda la hora jornal de las 09:00 horas hasta 22:30 horas, donde ese periodo de tiempo los usuarios reportan lentitud de acceso a la red y a los sistemas informáticos por la demanda del uso del tráfico de datos, generando retrasos de atención a los clientes, este escenario se presenta por no tener una gestión de control de ancho de banda y distribución de tráfico separando lo prioritario y no prioritario. Así, desencadenando desperdicio y mal uso del ancho de banda. Esta misma situación ocurre con las siguientes imágenes extraídas del reporte de las tiendas remotas, para esta estadística solo se tomó la muestra de dos tiendas, donde se registra el mismo comportamiento ocurrido en la oficina central. Se generó un reporte en el rango de horario de 09:00 horas hasta las 22:30 horas. El consumo fuerte se evidencia el inicio desde las 09:30 horas hasta el fin de la hora jornal, este comportamiento ocurre en todas las tiendas de la empresa, generando el malestar de los usuarios del área operativa.

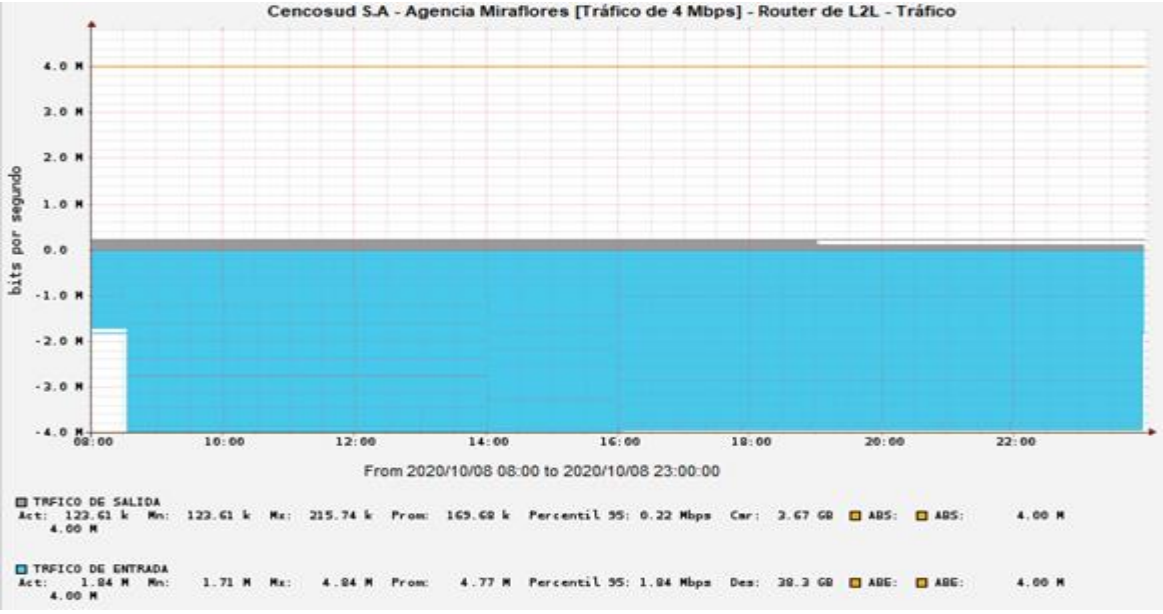


Figura 19. Tráfico de la Tienda Miraflores

Fuente: (Elaboración Propia, 2020)

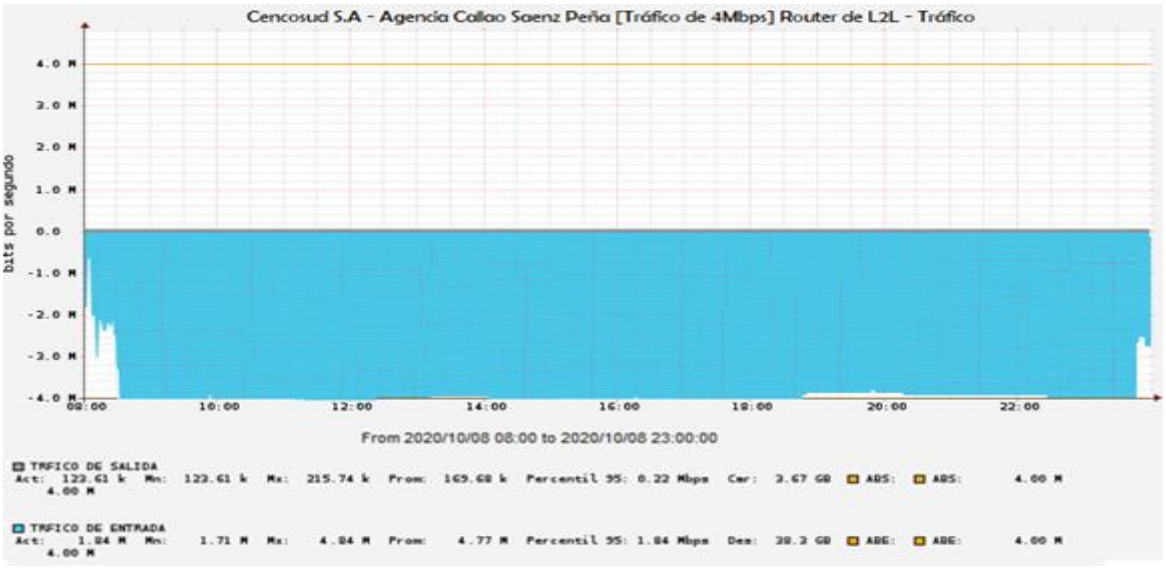


Figura 20. Tráfico de la Tienda Callao

Fuente: (Elaboración Propia, 2020)

4.1.1. Arquitectura Actual

Con relación al caso actual, se presenta la topología física a alto nivel. En líneas generales, para simplificar las 89 tiendas de la empresa solo se consideró en el diseño la Oficina Central más 3 tiendas remotas para la explicación del funcionamiento de la arquitectura de red, ya que se mantiene el mismo modelo de conexión física para cada sucursal. En la actualidad, la empresa cuenta con un servicio de Internet, Firewall más un enlace dedicado de L2L para la Oficina Central y un enlace de L2L para cada tienda remota. Donde, se establece la comunicación entre ellas por medio de la red MPLS a través de los protocolos de enrutamientos. Como se había mencionado anteriormente la empresa tiene distribuido un ancho de banda de 150 Mbps para la Oficina Central y un ancho de banda 4 Mbps por cada tienda remota, Por consiguiente, en el diseño solo se graficó los equipamiento lógicos y físicos de la oficina central y tres tiendas remotas para la

explicación del funcionamiento del flujo de tráfico de red y los accesos a los recursos de los sistemas y servidores de la oficina central como se visualiza en la siguiente imagen:

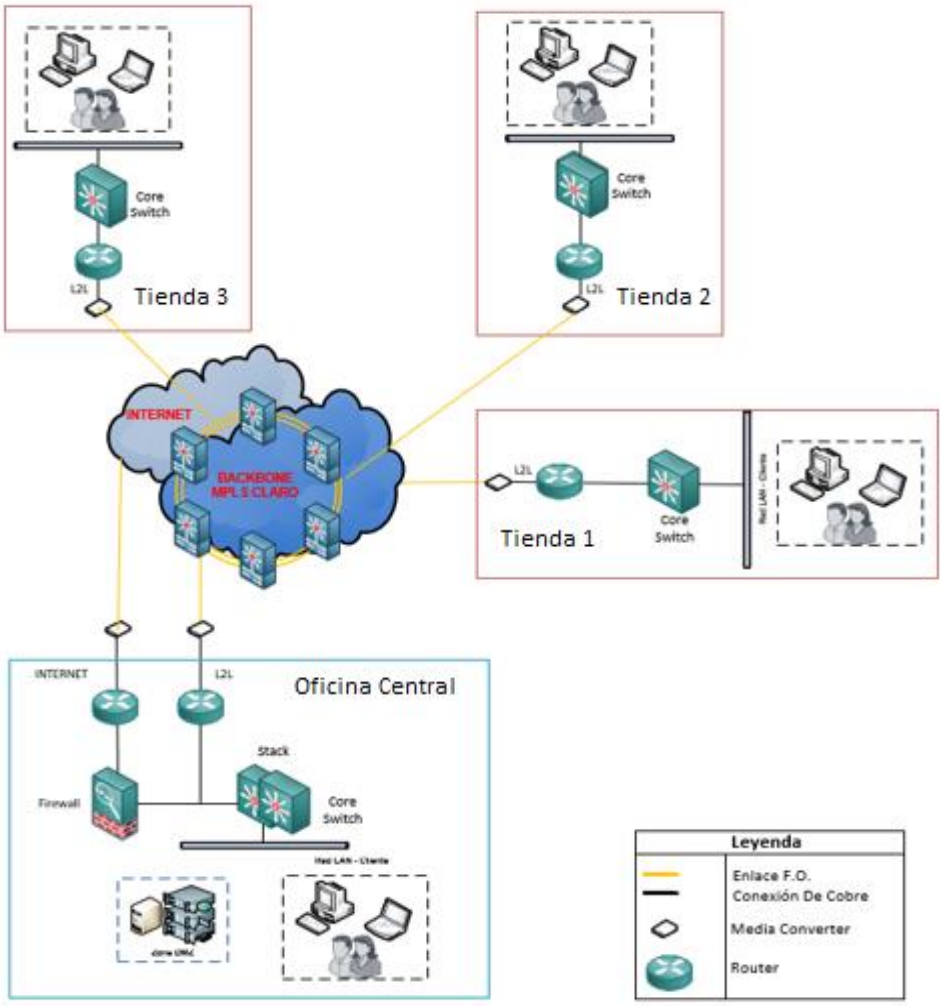


Figura 21. Arquitectura Actual

Fuente: (Elaboración Propia, 2020)

En resumen, se elaboró el diseño de la topología de red de la empresa Cencosud S.A, donde actualmente ocurre los problemas de congestionamiento y disponibilidad de la red, En primer lugar, en el funcionamiento de la comunicación de red, todas las peticiones de consultas y acceso a los sistemas de las tiendas remotas son recibido por el ruteador de

L2L de la oficina central donde se concentra toda la comunicación de datos para responder a todas las peticiones de origen. Es por ello, qué ante un evento externo no controlado como por ejemplo la avería del enlace de fibra óptica de L2L de la oficina central afectaría la disponibilidad de todas las comunicaciones de los enlaces de L2L, interrumpiendo drásticamente la productividad de la empresa. Consecuentemente, esto ocurre por no contar con un diseño de alta disponibilidad en el enlace de L2L de la oficina central que pueda reaccionar de forma eficiente ante cualquier falla en los enlaces dedicados representado en el gráfico por la línea de color amarillo. Por otro punto, los problemas de lentitud en la red, es ocasionado por el uso desmedido del ancho de banda afectando la comunicación de origen a destino denotado en los enlaces que intercomunica las tiendas remotas con la oficina central a través de la red de backbone de MPLS.

4.2. Desarrollo de la Aplicación de la Metodología Propuesta

4.2.1. Etapa 1 Preparación

Sobre la base del desarrollo de mejora, se aplicarán las sugerencias del caso propuesto presentado en el Capítulo 4 “Desarrollo de la Metodología Protocolo Secure SD-WAN”. Para ello, el mismo despliegue de este se llevará a cabo paso a paso, proporcionando el detalle de las fases de Diseño, Implementación, Operación y Optimización, con un enfoque en redes y comunicaciones. El propósito de este trabajo es poder brindar una solución que considere los objetivos técnicos y comerciales a adaptarse para brindar una gestión eficaz de una red con altos niveles de disponibilidad y seguridad. Adicional de proveer escalabilidad a la red mediante los nuevos servicios implementados que apoye a la mejora de la infraestructura de la red que permitan garantizar mayor

disponibilidad, mantener un óptimo monitoreo y permita establecer acciones contingentes ante posibles eventos; además de proporcionar datos a los requisitos de la unidad de control interno y los requisitos externos.

4.2.1.1. Propuesta Técnica.

Para la propuesta del Diseño del Protocolo Secure SD-WAN, se considerará las siguientes tecnologías de hardware y software para cumplir con todos los requisitos que se requiere para el funcionamiento óptimo de la solución. Se garantizará la viabilidad para la elaboración de un diseño disponible, escalable, seguro y eficaz para el mejor desempeño de la red de usuarios y brinde el funcionamiento de manera activa.

En el sentido de tecnología de hardware físico se utilizará

- **Fortigate 100 E:** El siguiente modelo de equipo será utilizado para la Oficina Central como ruteador en los enlaces de L2L para cubrir el escenario de alta disponibilidad y aplicar las configuraciones lógicas de SD-WAN. El equipo soporta un tráfico de 500 Mbps, 2000 túneles IPsec y 2 millones de sesiones concurrentes cubriendo la capacidad requerida para la solución propuesta.

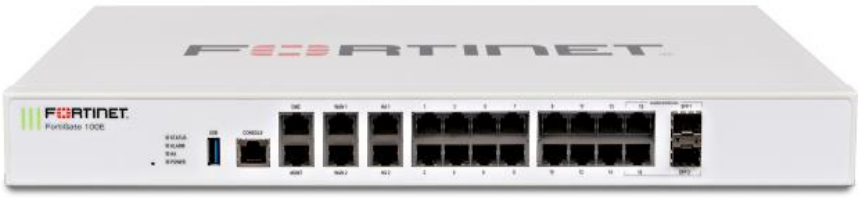


Figura 22. Equipo Fortigate 100E

Fuente: (Fortigate INC, 2020)

- **Fortigate 50E:** El siguiente modelo de equipo será utilizado para todas las tiendas remotas como ruteador de los enlaces de L2L y poder aplicar las configuraciones lógicas de SD-WAN para el balanceo de enlaces. El equipo soporta un tráfico de 250 Mbps y 1.5 millones de sesiones concurrentes con ranura de USB para la conexión de 4G, cubriendo así a capacidad requerida para la solución propuesta.

Figura 23. Equipo Fortigate 50E

Fuente: (Fortigate INC, 2020)

- **USB Módem – Huawei E8372:** El siguiente modelo propuesto será utilizado para brindar la segunda conexión en las tiendas remotas para aplicar el balanceo de enlaces para el tráfico de baja prioridad. El equipo soporta conexiones de 4G LTE y 3G dependiendo la cobertura de la zona.

Figura 24. USB Modem Huawei E8372

Fuente: (Huawei CORP, 2020)

- **Chips 4G:** Se gestionará la compra de Chips con plan de datos ilimitados para la colocación de los USB módem Huawei E8372 para cubrir la necesidad de alta disponibilidad de las tiendas remotas.

Figura 25. Chips 4G LTE

Fuente: (Alamy, 2019)

En el sentido de tecnología de hardware lógico se utilizará

- **Secure SD-WAN:** Proporcionará una manera inteligente de enrutar el tráfico crítico de WAN a través de ubicaciones distribuidas geográficamente. Las empresas que necesitan conectividad entre sus oficinas centrales, sucursales y centros de datos dependen de las ofertas de WAN, como líneas privadas y circuitos MPLS de sus proveedores de servicios. Brinda balanceo y contingencia del tráfico hacia el Datacenter principal a través de redes virtuales dinámicas y Optimiza el acceso a las aplicaciones.
- **ADVPN:** Es una configuración lógica que garantizará la seguridad de los datos que viajan a través del internet encriptando los datos de origen a destino. La comunicación se administra de forma dinámica y automática.

- **Protocolo de Enrutamiento BGP:** Protocolo de enrutamiento dinámico, utilizado para intercambiar información de enrutamiento entre diferentes prefijos en la red interna.
- **Traffic Shaping:** Técnica que se utilizará para controlar, priorizar y garantizar el rendimiento del ancho de banda en la comunicación de datos en una red donde exista problemas de congestionamiento de tráfico de datos.

En el sentido de tecnología de Software se utilizará.

- **PRTG:** Es una herramienta que monitorea LANs, WANs, servidores, aplicaciones etc. Potente y fácil de usar. Crea mapas individuales para identificar mediante sus sensores de medición para realizar seguimiento de las redes.
- **CACTI:** Esta es una solución para generar gráficos de red, diseñado para la visualización de capacidades y funciones de almacenamiento de datos con la finalidad de mostrar gráficos de alto nivel de medición de tráfico para determinar el consumo de ancho de banda, el tiempo de respuesta y la variación de la latencia.
- **GNS3:** Miles de ingenieros de redes de todo el mundo lo utilizan para simular, configurar, probar y solucionar problemas de redes virtuales y reales. GNS3 le permite ejecutar una pequeña topología que consta de solo unos pocos dispositivos en una computadora portátil, se pueden alojar hasta varios dispositivos en varios servidores o incluso dispositivos alojados en la nube.

- **VMware Workstation:** Es un software que se utiliza para ejecutar varios sistemas operativos como máquinas virtuales en una sola PC con Linux o Windows. Los profesionales de TI, los desarrolladores y las empresas confían en Workstation Pro para crear, probar o demostrar software en cualquier dispositivo, plataforma o nube.

4.2.2. Etapa 2 Planificación

4.2.2.1. Roles y Responsabilidades.

En esta actividad, se construirá la asignación de roles y responsabilidad representado en la Tabla 6 aplicado al modelo de matriz RACI que participará cada actor en una tarea dentro del desarrollo del proyecto. En la siguiente tabla se definirá la relación de cada uno.

Tabla 6

Elaboración de la Matriz RACI

Roles		Gerencia	Gestor de Proyecto	Ingeniero de Instalación	Analista de Instalación
Tareas	Preparación	A	R	I	I
	Planificación	A	R	I	I
	Diseño	A	R	I	I
	Implementación	I	A	R	I
	Operación	I	A	C	R
	Optimización	I	A	C	R

Nota: Se muestra la asignación de los Roles y Responsabilidades; Autoría propia.

4.2.3. Etapa 3 Diseño

4.2.3.1. Arquitectura de Red Propuesta.

En la arquitectura propuesta, se buscará mejorar el nivel de operación de la red a través de mecanismos inteligentes de balanceo de carga para la distribución del tráfico que nos permitirá controlar y optimizar la comunicación informática de la empresa Cencosud S.A. Esto se logra a partir del trabajo que realiza el protocolo Secure SD-WAN que provee funcionalidad de enrutamiento basado en la calidad de los enlaces donde se mide la latencia, pérdidas de paquetes y ruido o variación del paquete que viaja por la red de datos. Adicionalmente se brindará una capa de seguridad donde se garantizará la confiabilidad y la integridad de los paquetes para el intercambio de la comunicación de origen a destino. Los mecanismos de balanceo ofrecerán una red altamente disponible lo cual busca que la comunicación siempre este activa y en producción ante cualquier incidencia de los enlaces dedicados WANs de L2L. Para esto se seleccionará el uso de enlaces de red 4G que servirán como enlaces activos para el tráfico de menor prioridad permitiendo distribuir la carga del tráfico y aprovechar al máximo el canal de transmisión de datos para el uso del tráfico crítico que se marcará como prioritario. Para complementar la disponibilidad de la red en la Oficina Central se optará implementar un arreglo de alta disponibilidad (HA).

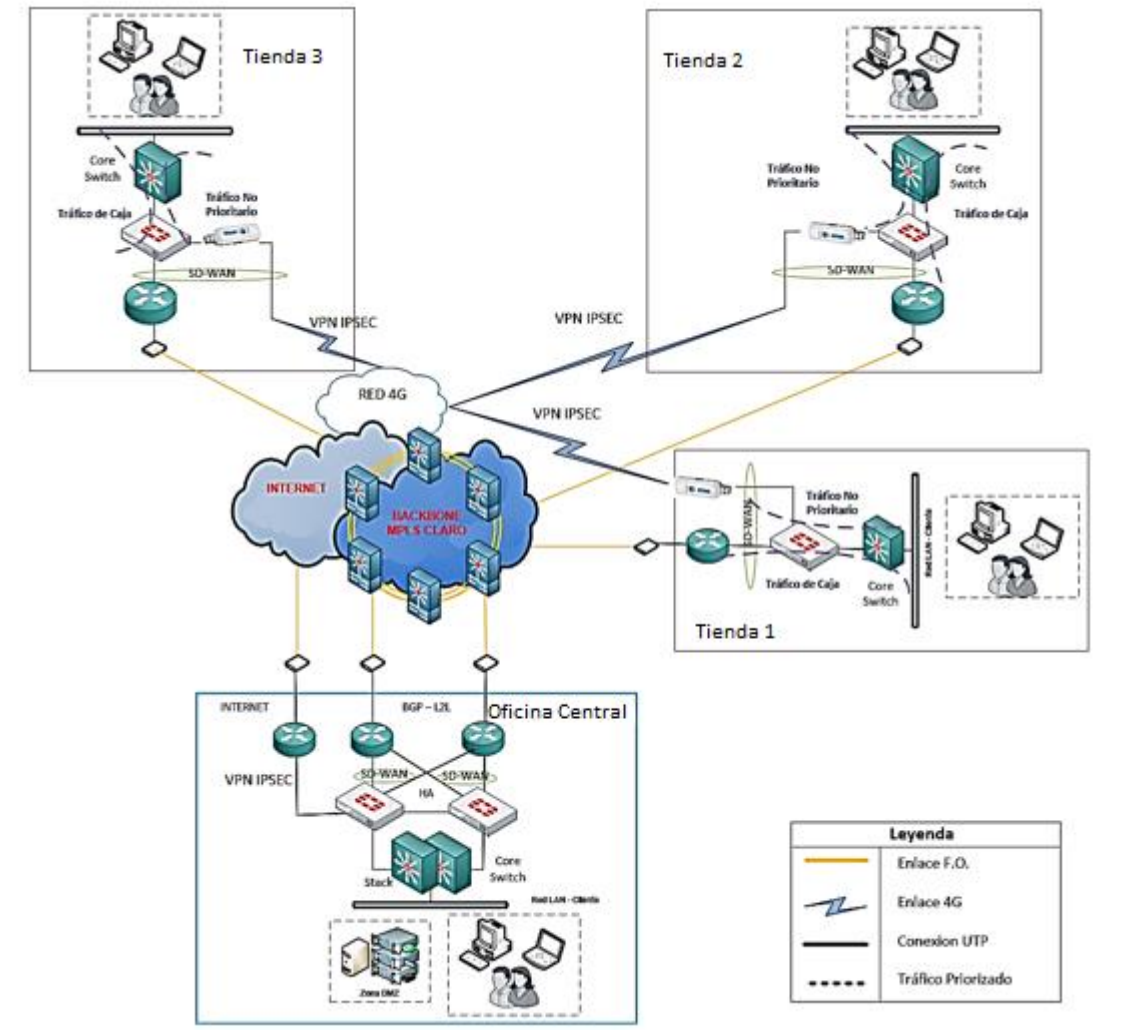


Figura 26. Arquitectura Propuesta

Fuente: (Elaboración Propia, 2020)

A continuación, se detalla el funcionamiento de la arquitectura propuesta para la mejora del congestionamiento y disponibilidad de red a través del diseño del protocolo de SD-WAN. Para el cumplimiento de esta solución, se habilitará en la oficina central un segundo enlace dedicado de L2L y la instalación de dos equipos Fortigate en Alta disponibilidad (HA), que brindará la función de Secure SD-WAN, a partir de este cambio todas las peticiones de comunicación de las tiendas remotas será respondido por medio de

los dos enlaces de L2L, es decir, en el caso ocurra una avería del primer enlace las consultas serán resueltas por el segundo enlace de L2L garantizando la disponibilidad del servicio. Asimismo, al disponer de dos enlaces dedicados, se aprovechará la capacidad de enlace para aumentar la disponibilidad del canal y discriminar el tráfico prioritario y no prioritario a través de las configuraciones de reglas SD-WAN. Por otro lado, en las tiendas remotas se instalará un equipo fortigate de la serie 50E que cumplirá la función de balanceo de enlace a través de SD-WAN para customizar los costos, se habilitará un enlace de 4G como un segundo enlace para discriminar los tráficos no prioritarios como la disponibilidad de enlace ante alguna avería o suceso externo que ocurra con el enlace dedicado de fibra óptica. Por último, se añadirá valores agregados a la solución para garantizar la seguridad, integridad y confiabilidad de los datos que viajen por el enlace de internet de 4G, como la configuración de ADVPN para la encriptación de datos de forma dinámica y segura con el fin de evitar cualquier robo o alteración de la información de la empresa. Asimismo, se habilitará la configuración de traffic shaping para crear colas de prioridad con el fin de tener un control y gestión del ancho de banda de todas las tiendas y evitar congestionamiento de red, logrando a los usuarios tener una mejor experiencia con el acceso a los sistemas informáticos.

4.2.3.2. Arquitectura de la simulación.

Para la simulación del desarrollo de la implementación, se utilizará como prueba de concepto el siguiente esquema de red orientado a la arquitectura propuesta donde se sustentará y se demostrará los beneficios del protocolo Secure SD-WAN.

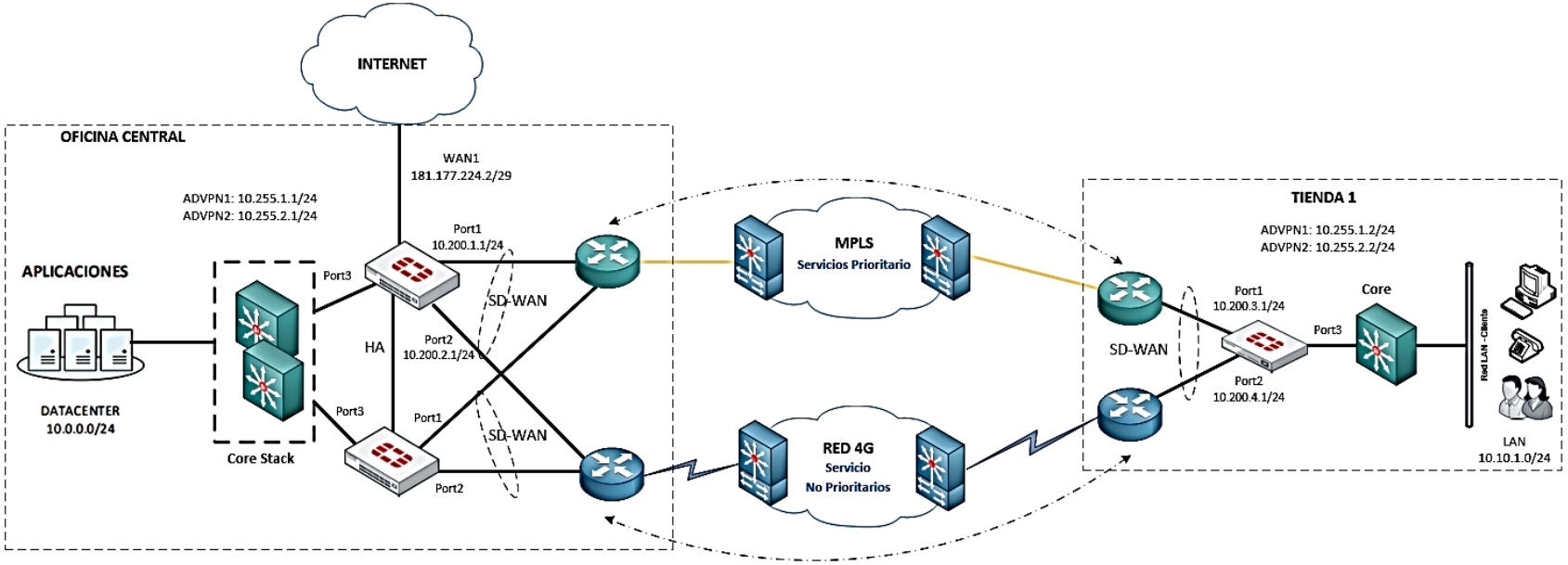


Figura 27. Arquitectura de Simulación

Fuente: (Elaboración Propia, 2020)

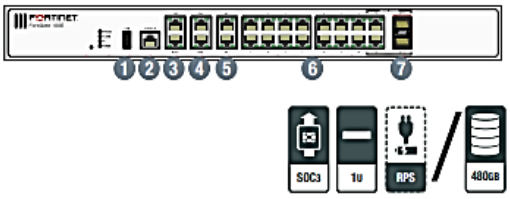
En referencia al punto 4.3.2.1 “Arquitectura de Red Propuesta Actual”, se simplificará el diseño de la red propuesta, el cual solo se habilitará la simulación de la oficina central con una tienda remota ya que cubre la necesidad para las pruebas de Secure SD-WAN. Entonces para el protocolo de pruebas, se creará la virtualización de los dos equipos Fortigate de la oficina central en una arquitectura de alta disponibilidad (HA) para la simulación de los dos enlaces dedicados a través del protocolo Secure SD-WAN y el arreglo para la disponibilidad a nivel de hardware. Asimismo, se habilitará las configuraciones de ADVPN para la seguridad, confiabilidad e integridad de datos como la segmentación de tráfico para clasificar los datos a través de prioridades de colas para brindar una control, distribución y gestión del ancho de banda de todas las tiendas y subsanar los problemas de congestionamiento de red. Para esta solución se utilizará los programas de simulación de red GNS3 y virtualización de sistemas operativos a través del software VMware.

4.2.3.1. Arquitectura de Hardware de los equipos propuestos.

- **Fortigate 100E Series:** La serie FortiGate 100E proporciona una solución SD-WAN segura, escalable y centrada en la aplicación con capacidades de firewall de próxima generación (NGFW) para medianas y grandes empresas implementadas en el campus o nivel de sucursal empresarial. Protege contra las amenazas cibernéticas con aceleración del sistema en un chip y mecanismo inteligentes de SD-WAN.

Hardware

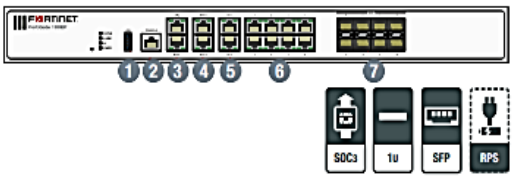
FortiGate 100E/101E



Interfaces

1. USB Port
2. Console Port
3. 2x GE RJ45 MGMT/DMZ Ports
4. 2x GE RJ45 WAN Ports
5. 2x GE RJ45 HA Ports
6. 14x GE RJ45 Ports
7. 2x GE RJ45/SFP Shared Media Pairs

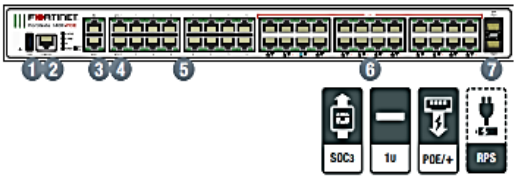
FortiGate 100EF



Interfaces

1. USB Port
2. Console Port
3. 2x GE RJ45 MGMT/DMZ Ports
4. 2x GE RJ45 WAN Ports
5. 2x GE RJ45 HA Ports
6. 8x GE RJ45 Ports
7. 8x GE SFP Slots

FortiGate 140E-POE



Interfaces

1. USB Port
2. Console Port
3. 2x GE RJ45 MGMT/HA Ports
4. 2x GE RJ45 WAN Ports
5. 14x GE RJ45 Ports
6. 24x GE RJ45 POE Ports
7. 2x GE SFP DMZ Slots

Figura 28. Hardware del equipo Fortigate 100E

Fuente: (Fortinet INC, 2020)

- **Fortigate 50E Series:** La serie FortiGate / FortiWiFi 50E proporciona una solución SD-WAN segura, escalable y centrada en la aplicación en un factor de forma de escritorio compacto sin ventilador para sucursales empresariales y empresas medianas. Protege contra las amenazas cibernéticas con aceleración del sistema en un chip y mecanismo inteligentes de SD-WAN.

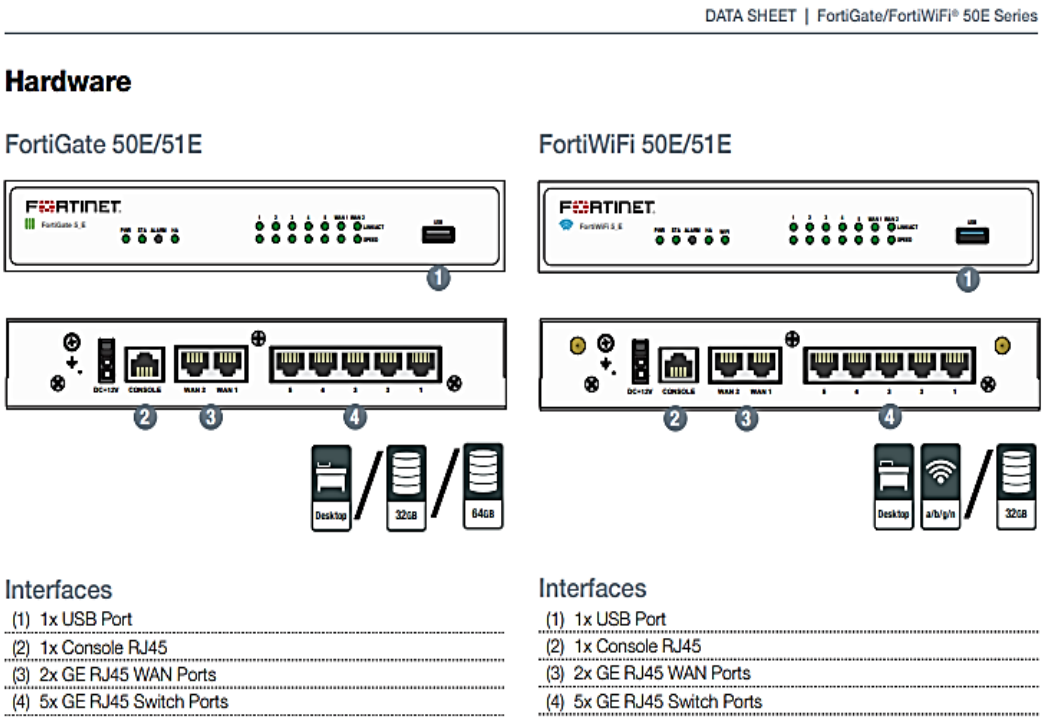


Figura 29. Hardware del equipo Fortigate 50E

Fuente: (Fortinet INC, 2020)

4.2.4. Etapa 4 Implementación

4.2.4.1. Simulación del diseño de red.

Una vez provisto el diseño de red. A continuación, se comenzará con las pruebas de concepto que permitirá efectuar una simulación mediante la herramienta GN3 que permitirá validar todas las funcionalidades y característica del diseño del protocolo Secure SD-WAN para su óptimo funcionamiento de la solución propuesta.

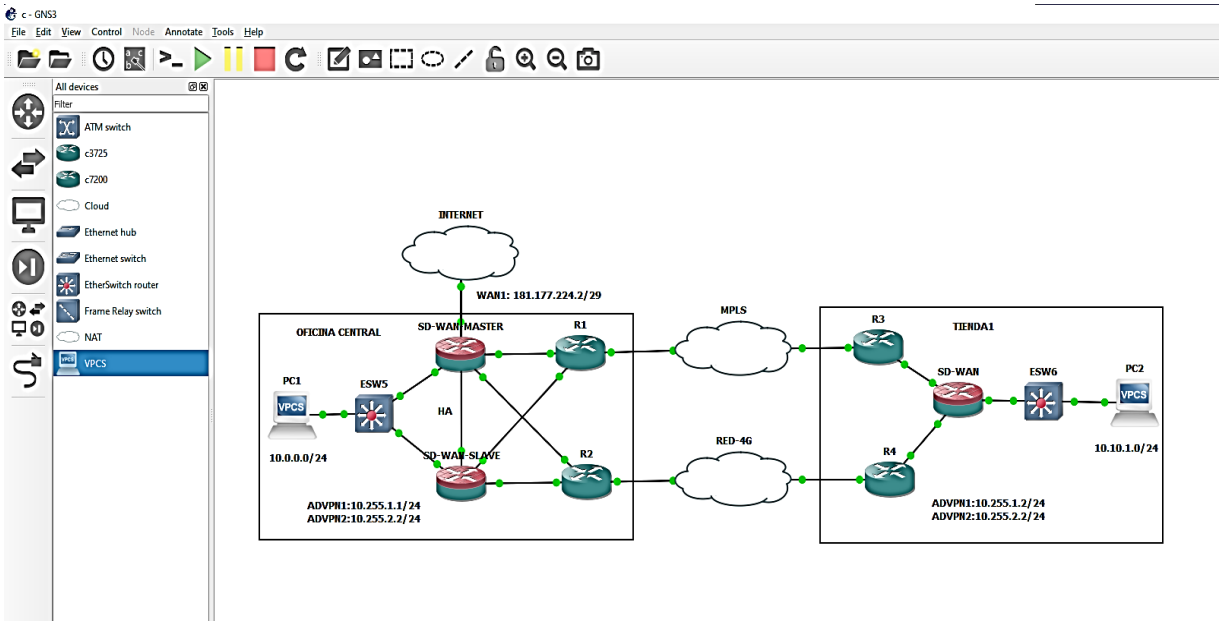


Figura 30. Herramienta de Simulación GNS3

Fuente: (Elaboración Propia, 2020)

De acuerdo con el diseño explicado en el punto 4.2.3.2. “Arquitectura de la simulación”, se traslada el diseño elaborado en la herramienta de GNS3 para dar el inicio a las pruebas de simulación del protocolo de Secure SD-WAN. Asimismo, la herramienta será integrada con el software VMware para la instalación de los sistemas operativos que simulará al funcionamiento de los equipos Fortigate.

4.2.4.2. Virtualización.

Una vez provista la solución de software se procederá con la virtualización de los equipos firewall fortigate que brindará la solución de Secure SD-WAN para las pruebas de concepto. Las pruebas se limitan a la administración de los recursos motivo por el cual las pruebas se garantizará sobre la comunicación de la Oficina Central y la tienda 1 haciendo la réplica de una sucursal de la infraestructura de Cencosud S.A. Para la virtualización del equipo se trabajará con el software VMware que ofrece la virtualización en un ambiente controlado, donde se cargará la imagen ISO del sistema de Fortigate para la habilitación de control de pruebas y de forma seguida se configurará la máquina virtual con los siguientes recursos: CPU (1), Memoria RAM (1 Gbps), Disco Duro (512 Mbps).

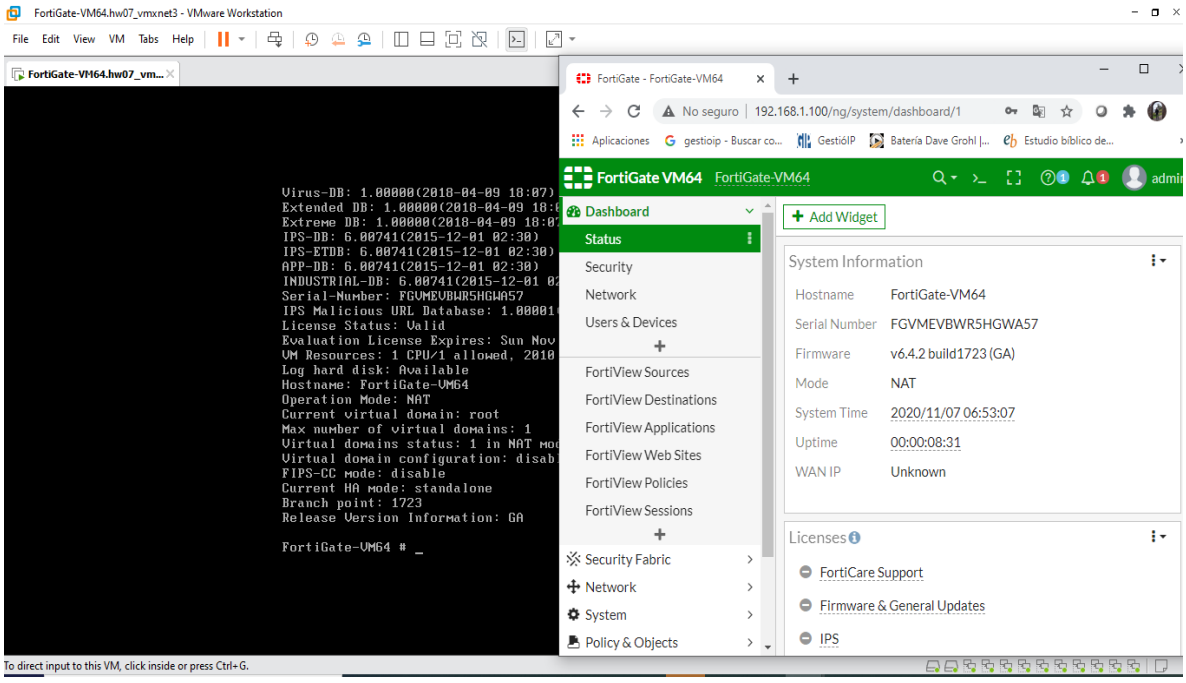


Figura 31. Herramienta de Virtualización VMware

Fuente: (Elaboración Propia, 2020

4.2.4.3. Configuración de HA.

A continuación, se detalla la función de Alta Disponibilidad (HA) configurado en la Oficina Central que garantizará la contingencia de equipamiento a nivel de hardware ante cualquier falla o avería del equipo principal. Se define la prioridad mayor para declarar el equipo que se comportará como el principal en la red. Asimismo, se habilitará el monitoreo de las interfaces físicas del equipo para censar el estado de los enlaces que participará en la comunicación de la red con la finalidad que ante cualquier caída del enlace el equipo responda la solicitud de contingencia.

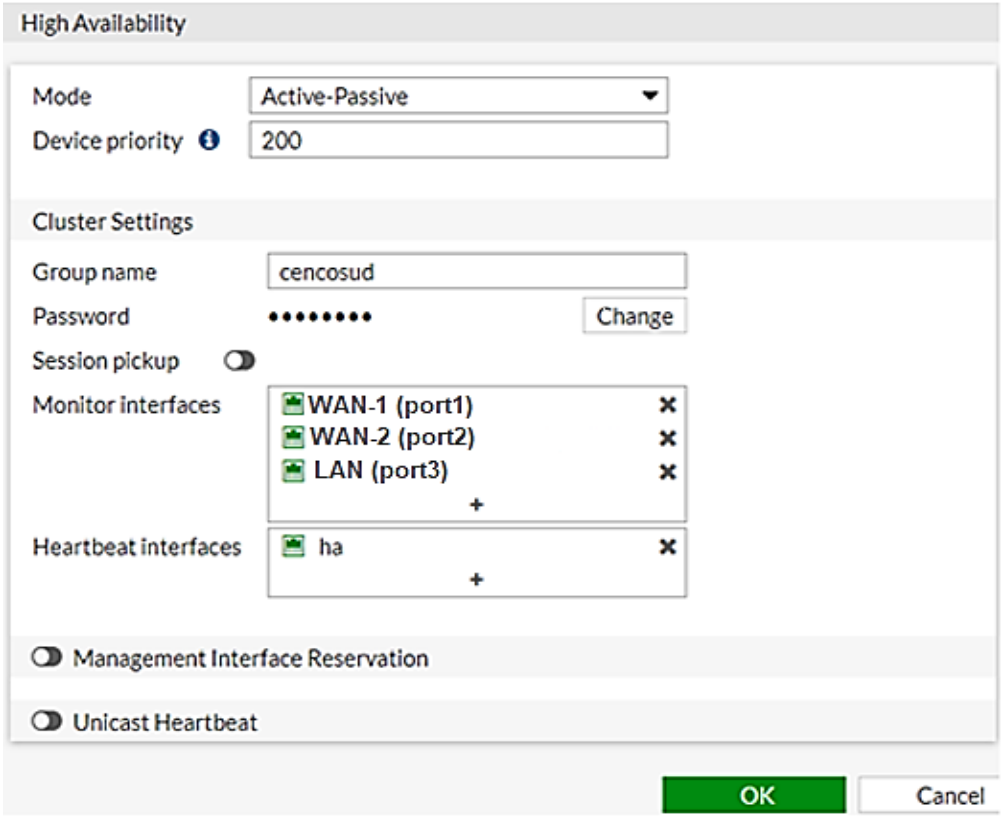


Figura 32. Configuración de HA Equipo Principal

Fuente: (Elaboración Propia, 2020)

Se declara la prioridad del equipo secundario el cual debe ser menor al equipo principal para el funcionamiento de roles de Alta Disponibilidad.

Figura 33. Configuración de HA Equipo Secundario

Fuente: (Elaboración Propia, 2020)

En la siguiente imagen se visualizará el estado de funcionamiento del arreglo de Alta Disponibilidad del equipo SD-WAN de la Oficina Central donde se define el rol de acuerdo con la configuración de prioridades asignadas a cada equipo Fortigate.

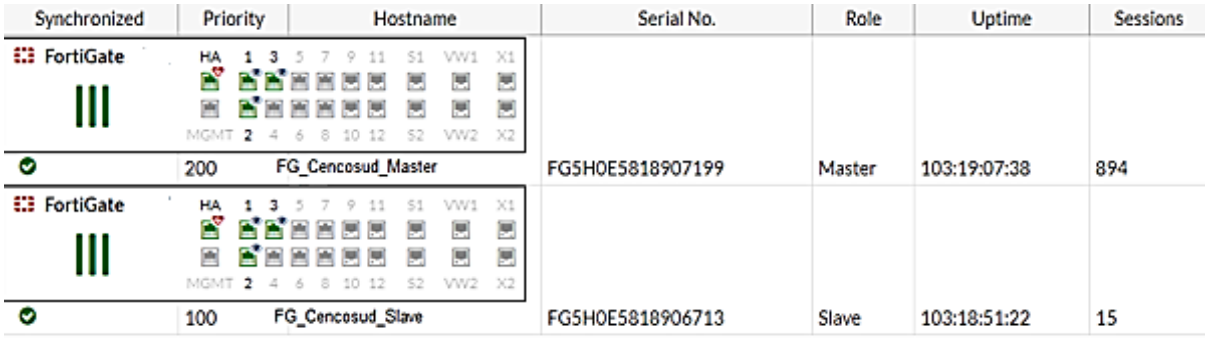


Figura 34. Estado del arreglo de HA

Fuente: (Elaboración Propia, 2020)

4.2.4.4. Configuración de Interfaces.

Una vez integrado el arreglo de alta disponibilidad del equipamiento Fortigate de la Oficina Central se procederá con las configuraciones de las interfaces físicas donde se asignará el direccionamiento IP definido en la Etapa III de Diseño expuesta en el diagrama de Arquitectura de Simulación. Esta etapa se configurará tanto en los equipos de la Oficina Central como el de la Tienda 1.

4.2.4.4.1. Oficina Central.

Se asignará las siguientes direcciones IP para las interfaces del equipo.

- Puerto 1: 10.200.1.1/24 (WAN1)
- Puerto 2: 10.200.2.1/24 (WAN2)
- Puerto 3: 10.0.0.1/24 (LAN)

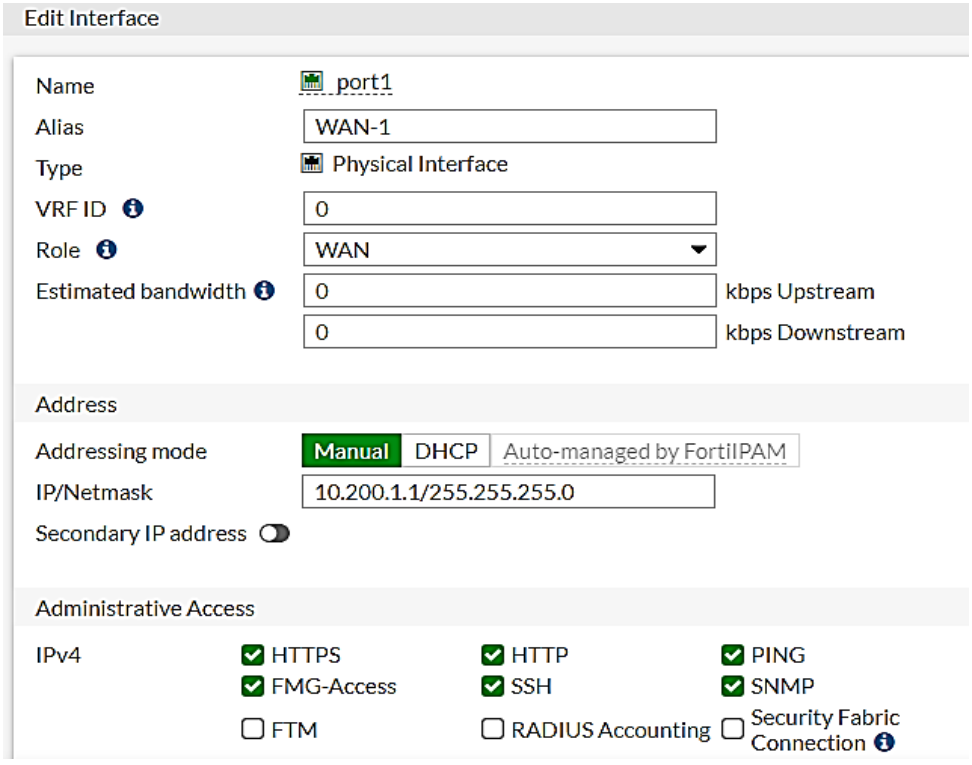


Figura 35. Interfaz Enlace WAN 1

Fuente: (Elaboración Propia, 2020)

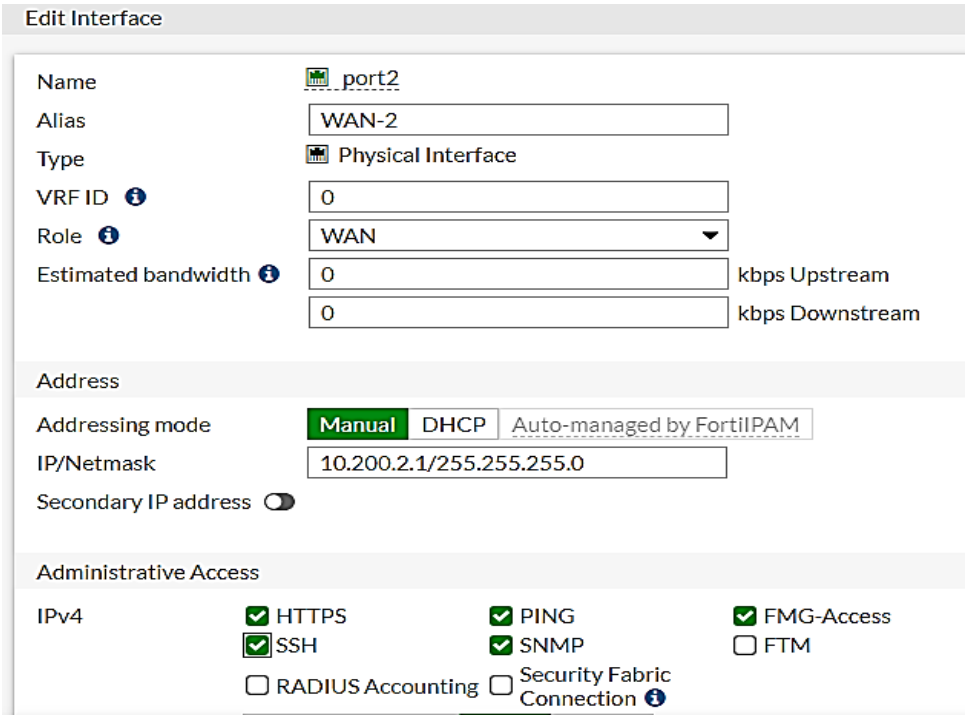


Figura 36. Interfaz Enlace WAN 2

Fuente: (Elaboración Propia, 2020)

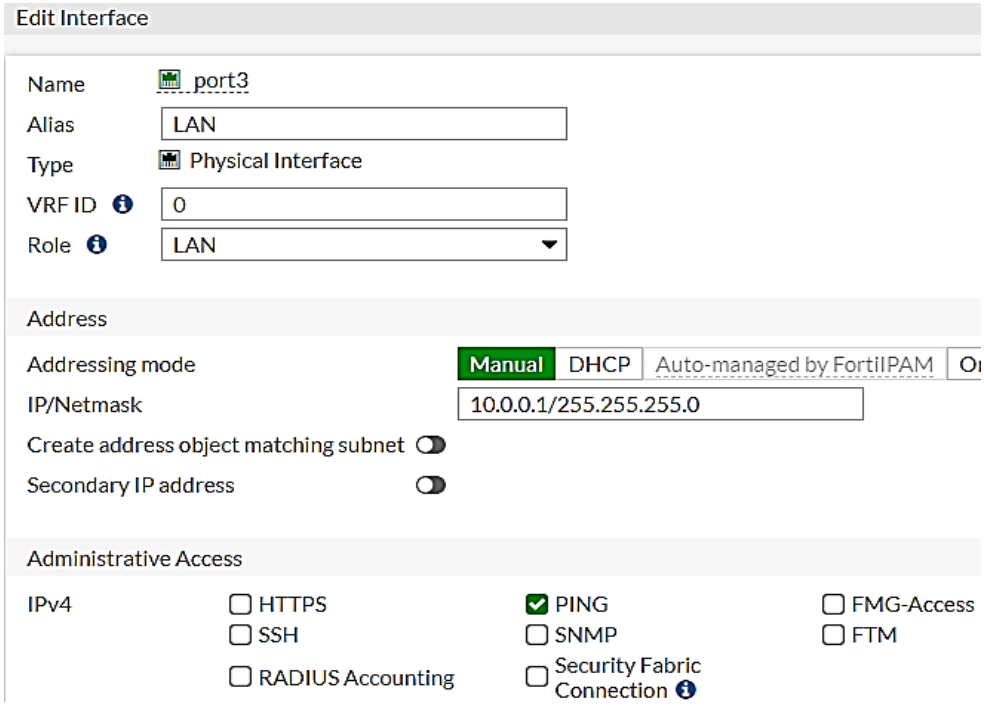


Figura 37. Interfaz Enlace LAN

Fuente: (Elaboración Propia, 2020)

4.2.4.4.2. Tienda 1.

Se asignará las siguientes direcciones IP para las interfaces del equipo Fortigate de la Tienda 1.

- Puerto 1: 10.200.1.2/24 (Enlace Prioritario)
- Puerto 2: 10.200.2.2/24 (Enlace No Prioritario)
- Puerto 3: 10.10.1.1/24 (LAN)

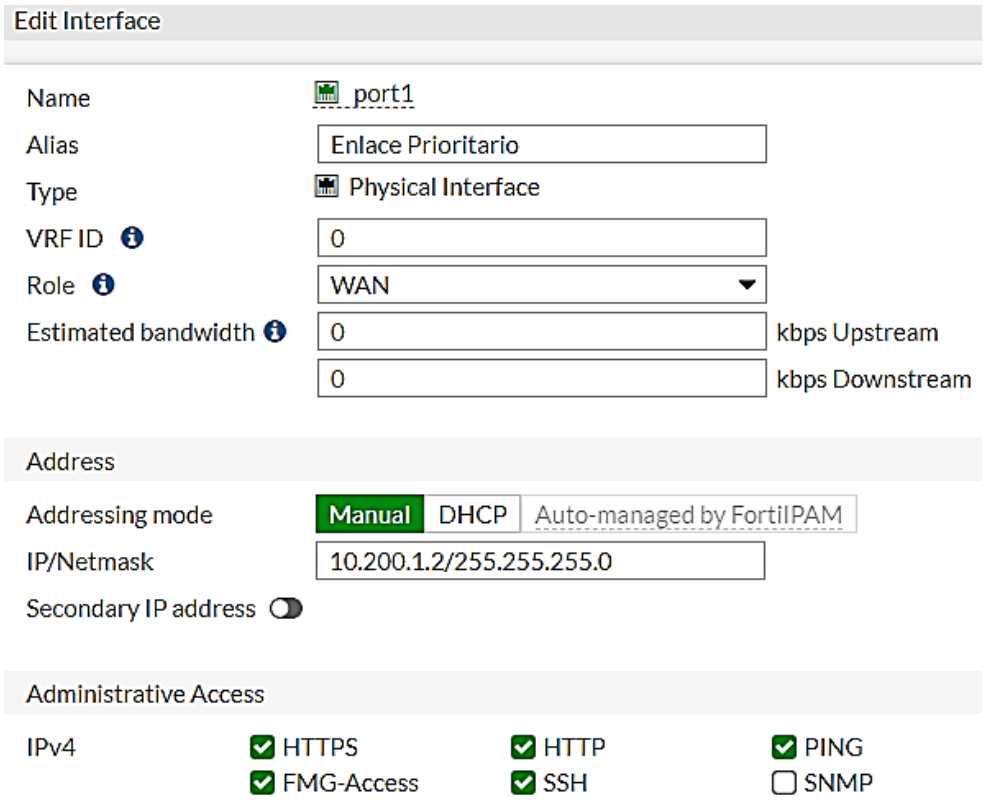


Figura 38. Interfaz Enlace Prioritario

Fuente: (Elaboración Propia, 2020)

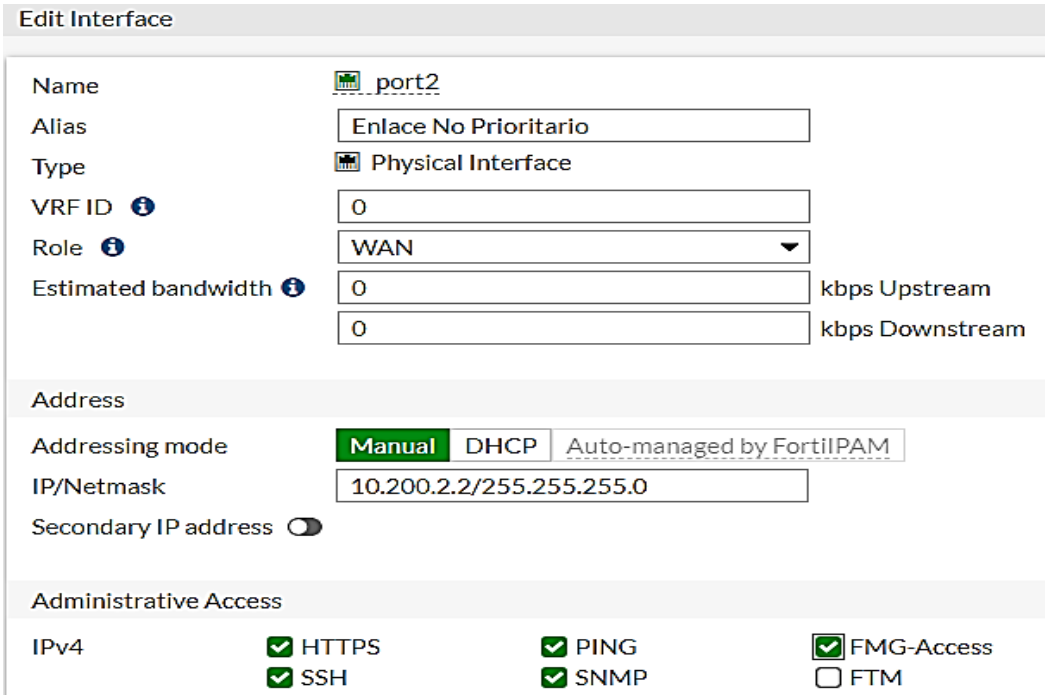


Figura 39. Interfaz Enlace No Prioritario

Fuente: (Elaboración Propia, 2020)

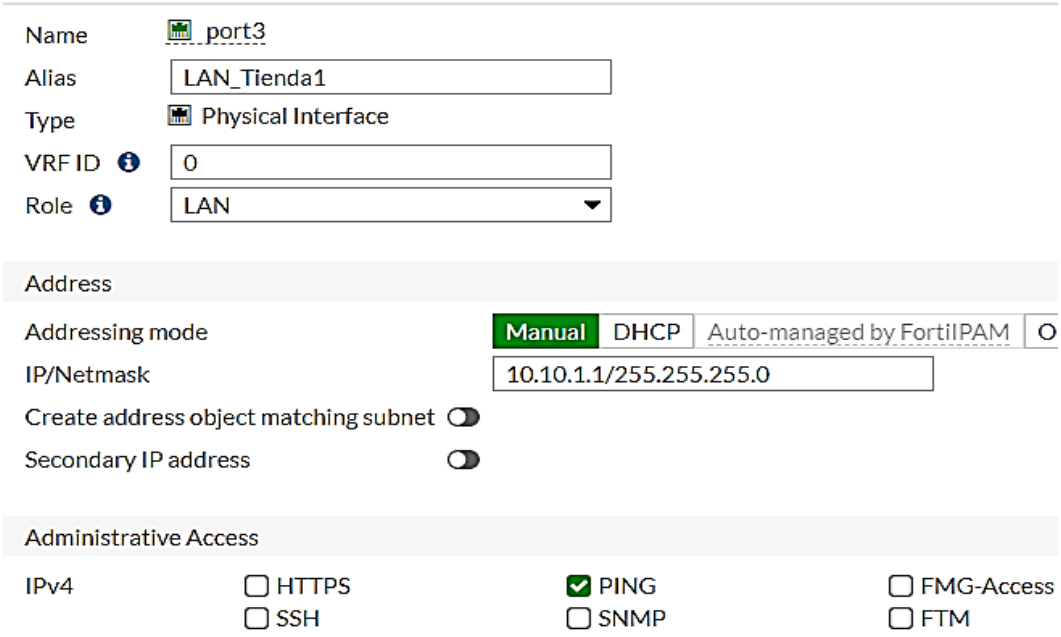
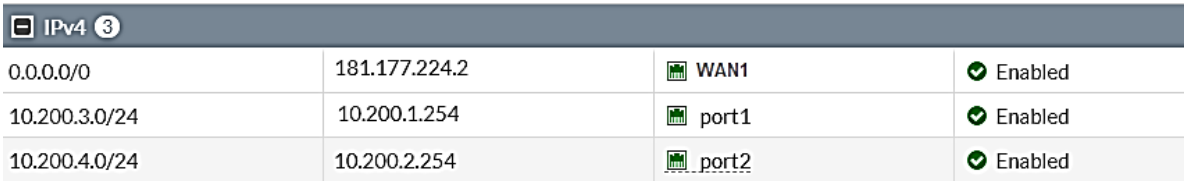


Figura 40. Interfaz Enlace LAN Tienda 1

Fuente: (Elaboración Propia, 2020)

4.2.4.5. Configuración de Enrutamiento.

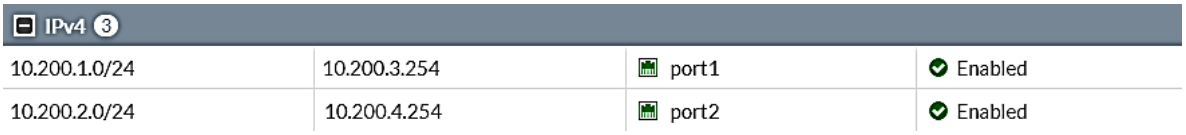
Por consiguiente, para establecer la comunicación entre los prefijos definidos en las interfaces WANs de los equipamientos es necesario habilitar el enrutamiento estático con el objetivo de configurar posteriormente el enrutamiento dinámico para las redes LANs por medio del protocolo BGP.



IPv4 3			
0.0.0.0/0	181.177.224.2	WAN1	Enabled
10.200.3.0/24	10.200.1.254	port1	Enabled
10.200.4.0/24	10.200.2.254	port2	Enabled

Figura 41. Tabla de Enrutamiento estático de la Oficina Central

Fuente: (Elaboración Propia, 2020)



IPv4 3			
10.200.1.0/24	10.200.3.254	port1	Enabled
10.200.2.0/24	10.200.4.254	port2	Enabled

Figura 42. Tabla de Enrutamiento estático de la Tienda 1

Fuente: (Elaboración Propia, 2020)

4.2.4.6. Configuración de ADVPN IPsec.

A continuación, se procederá con la habilitación de la configuración de ADVPN para la encriptación de los datos que viajan en la comunicación de transmisión de datos con el fin de brindar una capa adicional de seguridad como valor agregado a la solución de SD-WAN.

4.2.4.6.1. Configuración de Fase 1.

Para esta fase se definirá la conexión de la red privada virtual mediante On-Idle. Asimismo, se configurará la interfaz de salida como la WAN1 y la clave pre compartida para establecer el canal seguro para intercambio de llave entre las Oficinas para que los datos viajen de forma confiable, integra y segura. Para el desarrollo de la Fase 1, se habilitará el Dial UP User para la Oficina Central y Static IP en la Tienda1.

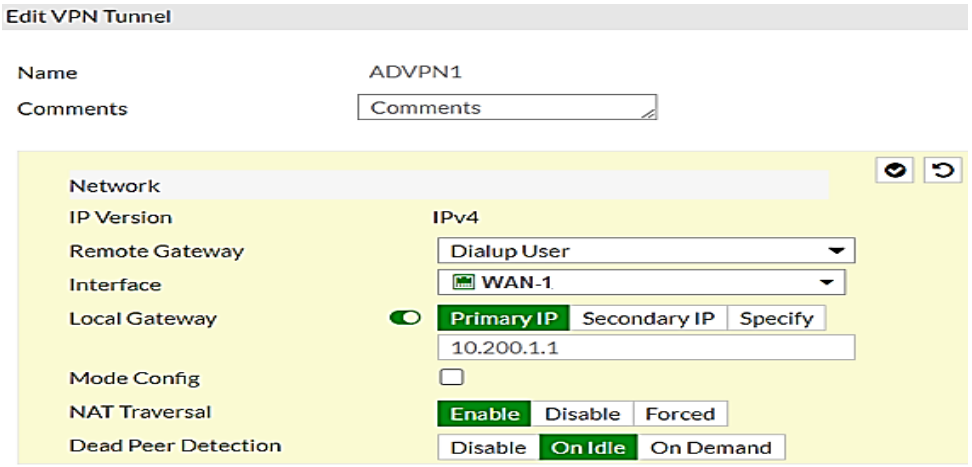


Figura 43. Configuración ADVPN fase 1 Oficina Central

Fuente: (Elaboración Propia, 2020)

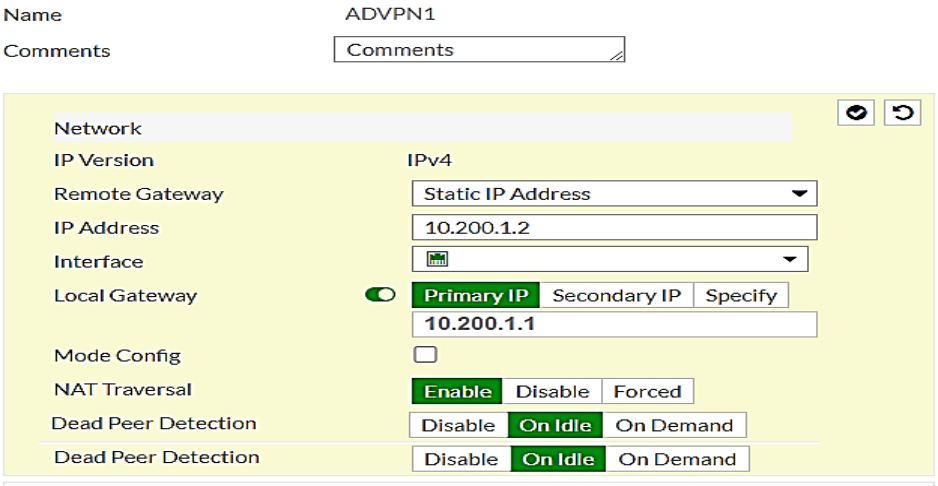


Figura 44. Configuración ADVPN fase 1Tienda 1

Fuente: (Elaboración Propia, 2020)

La contraseña de la llave pre compartida deberá se la misma en ambos extrema para la correcta negociación de la fase 1 de la ADVPN.

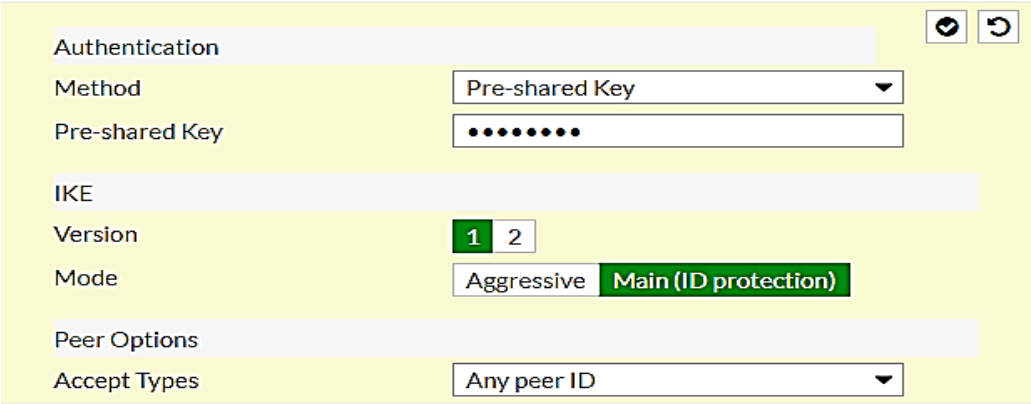


Figura 45. Configuración de la llave precompartida

Fuente: (Elaboración Propia, 2020)

En la siguiente imagen se observará la declaración de la encriptación y la autenticación que se usará para el establecimiento de la ADVPN, los parámetros de configuración deberán ser igual al otro extremo.

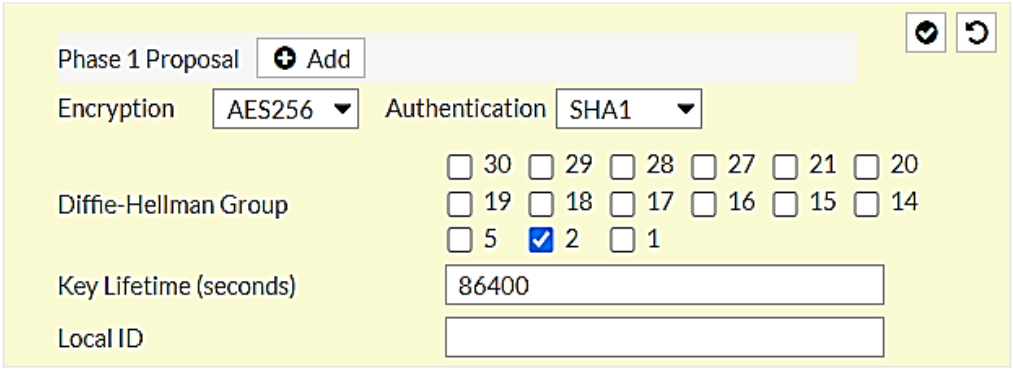


Figura 46. Configuración de encriptación y autenticación de fase 1

Fuente: (Elaboración Propia, 2020)

4.2.4.6.2. Configuración de Fase 2.

Para la configuración de la fase 2 se deberá definir las redes de comunicación como la encriptación, autenticación y el tiempo de vida de la llave considerar que toda configuración deberá ser igual al otro extremo donde se establecer la sesión de ADVPN.

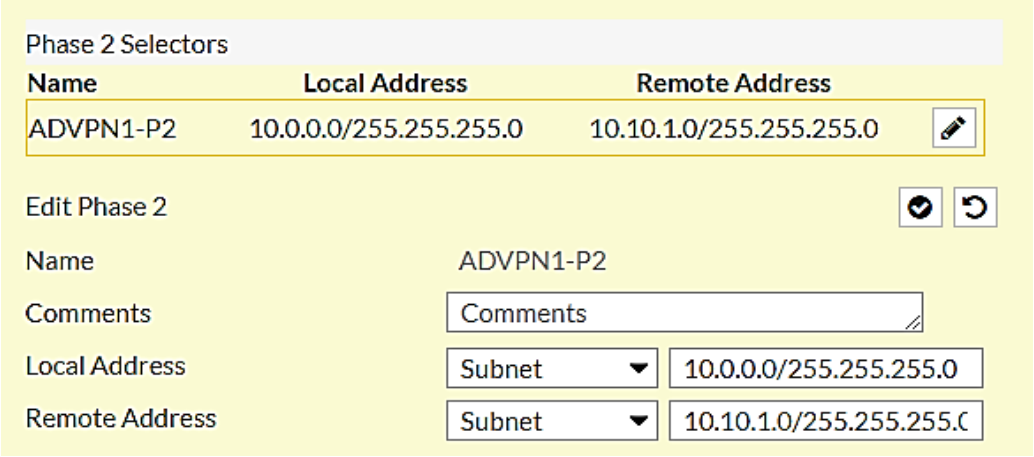


Figura 47. Configuración ADVPN fase 2 Agencia Central

Fuente: (Elaboración Propia, 2020)

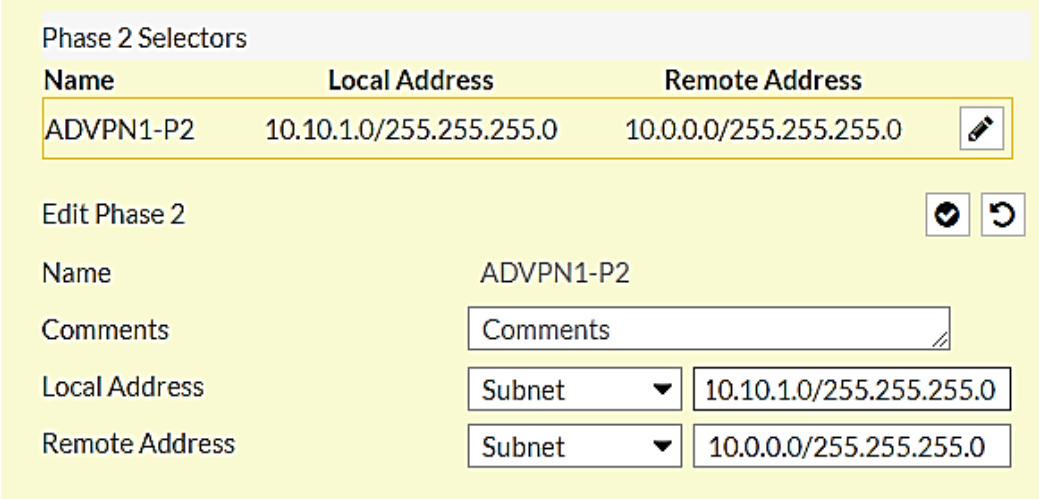


Figura 48. Configuración ADVPN fase 2 Tienda 1

Fuente: (Elaboración Propia, 2020)

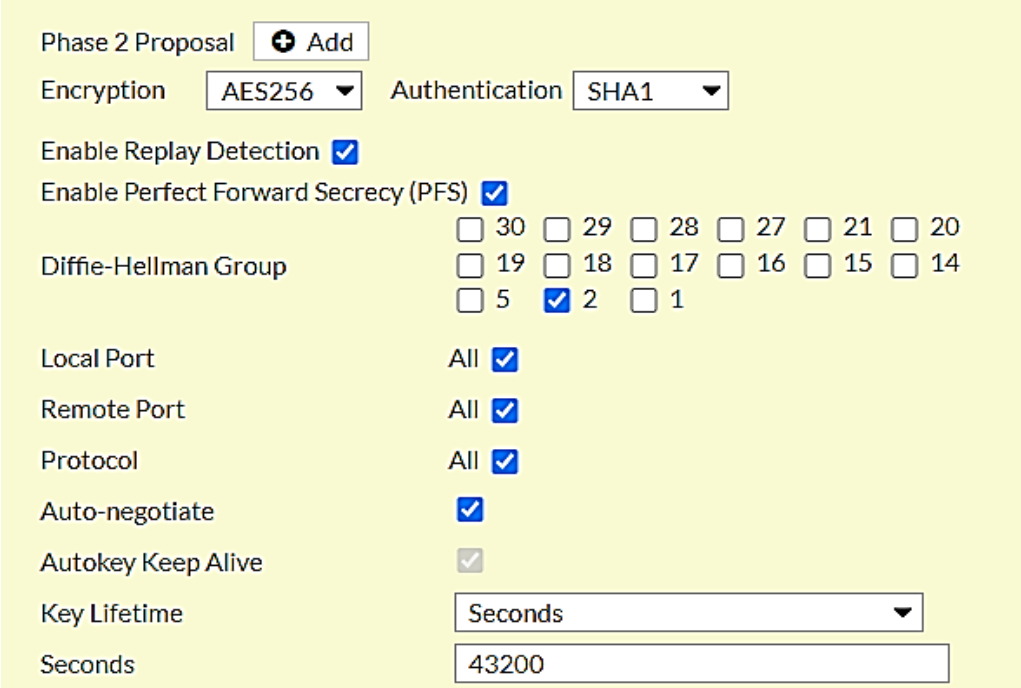


Figura 49. Configuración de Encriptación y Autenticación de fase 2

Fuente: (Elaboración Propia, 2020)

Asimismo, se definirá las direcciones IP para las interfaces ADVPN para el establecimiento de la comunicación de los túneles ADVPN IPsec. Se asignará los siguientes prefijos.

- ADVPN1 Oficina Central: 10.255.1.1
- ADVPN2 Oficina Central: 10.255.2.1
- ADVPN1 Tienda1: 10.255.1.2
- ADVPN2 Tienda1: 10.255.2.2

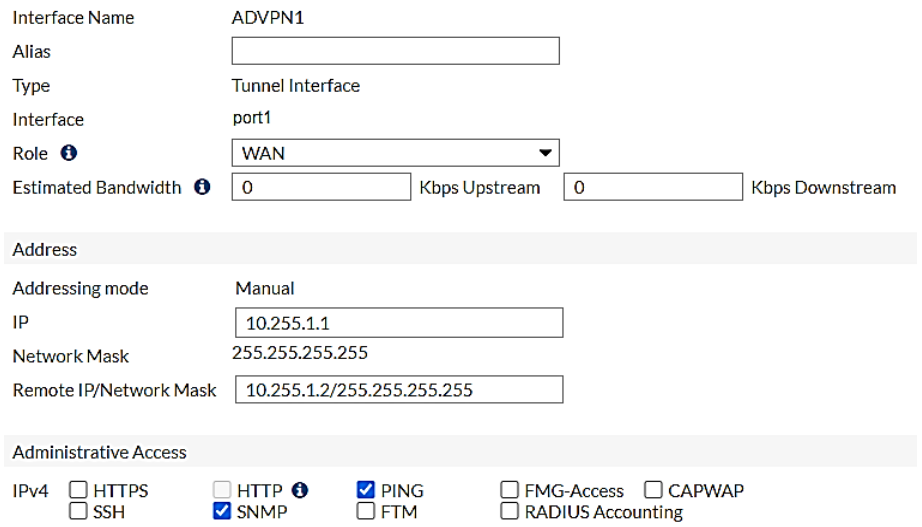


Figura 50. Configuración de IP ADVPN1 de la Oficina Central

Fuente: (Elaboración Propia, 2020)

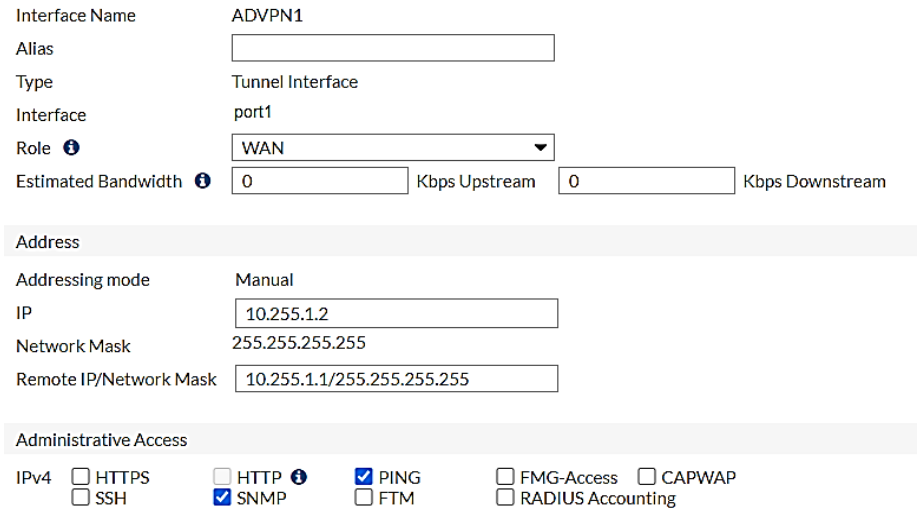


Figura 51. Configuración de IP ADVPN1 de la Tienda 1

Fuente: (Elaboración Propia, 2020)

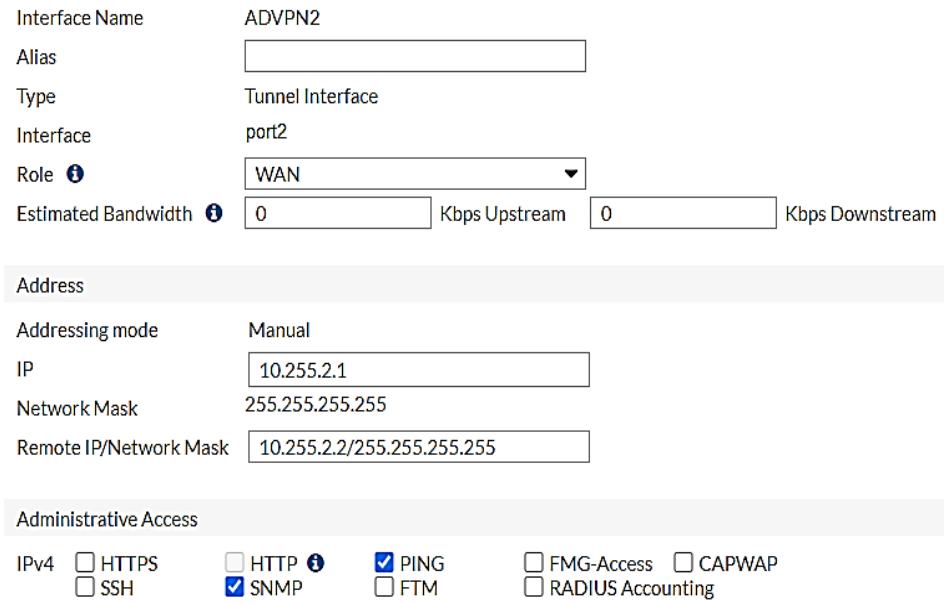


Figura 52. Configuración de IP ADVPN2 de la Oficina Central

Fuente: (Elaboración Propia, 2020)

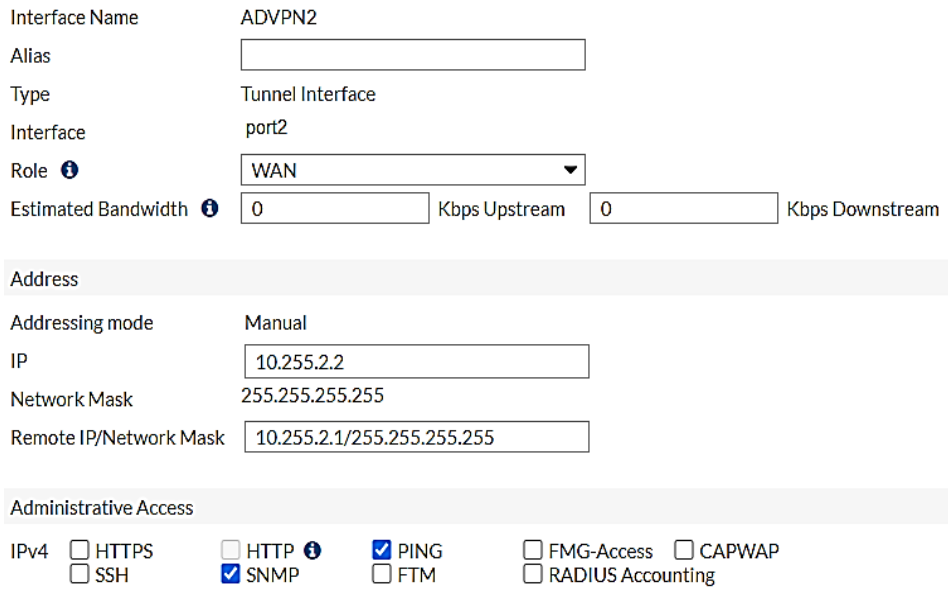


Figura 53. Configuración de IP ADVPN2 de la Tienda 1

Fuente: (Elaboración Propia, 2020)

4.2.4.7. Configuración de BGP y Prefix List.

En base a las consideraciones del escenario implementado, se optará configurar el enrutamiento dinámico para establecer el balanceo de rutas y caminos mediante el multihoming de aprendizaje ante la falla de los cualquiera de enlaces de transmisión de datos. Para ser posible este mecanismo de ruta se ha implementado el enrutamiento por BGP afinando la comunicación mediante lista de prefijos.

```
config router bgp
    set as 65000
    set router-id 10.200.1.1
    set keepalive-timer 1
    set holdtime-timer 3
    set ibgp-multipath enable
    set scan-time 5
    config neighbor-group
        edit "ADVPN1-PEERS"
            set advertisement-interval 1
            set capability-default-originate enable
            set link-down-failover enable
            set next-hop-self enable
            set soft-reconfiguration enable
            set default-originate-routemap "RM_DEFAULT"
            set remote-as 65000
            set route-map-in "entrada"
            set route-map-out "Anuncio"
            set route-reflector-client enable
        next
        edit "ADVPN2-PEERS"
            set advertisement-interval 1
            set capability-default-originate enable
            set link-down-failover enable
            set next-hop-self enable
            set soft-reconfiguration enable
            set default-originate-routemap "RM_DEFAULT"
            set remote-as 65000
            set route-map-in "entrada"
            set route-map-out "Anuncio"
            set route-reflector-client enable
        next
    end
```

Figura 54. Configuración de BGP de la Oficina Central

Fuente: (Elaboración Propia, 2020)

A través de la configuración de vecindad anunciamos los prefijos locales para inyectar las rutas al equipo del otro extremo Tienda 1 para la comunicación de ADVPN lo cual es necesario para el procedimiento de balanceo por SD-WAN.

```
config neighbor-range
    edit 1
        set prefix 10.255.1.0 255.255.255.0
        set neighbor-group "ADVPN1-PEERS"
    next
    edit 2
        set prefix 10.255.2.0 255.255.255.0
        set neighbor-group "ADVPN2-PEERS"
    next
end
```

Figura 55. Configuración de Vecindad BGP

Fuente: (Elaboración Propia, 2020)

```
config router prefix-list
    edit "PL_DEFAULT"
        config rule
            edit 1
                set prefix 0.0.0.0 0.0.0.0
                unset ge
                unset le
            next
        end
```

Figura 56. Configuración de prefix list

Fuente: (Elaboración Propia, 2020)

```
config router route-map
    edit "RM_DEFAULT"
        config rule
            edit 1
                set match-ip-address "PL_DEFAULT"
            next
        end
```

Figura 57. Configuración de router map

Fuente: (Elaboración Propia, 2020)

Asimismo, se configurará el enrutamiento por BGP en la tienda 1, lo cual se definirá la vecindad con la Oficina Central anunciando el prefijo de la red LAN 10.10.1.0/24, el número de sistema autónoma será el 65000 para la negociación entre los extremos para el compartimiento de la tabla de enrutamiento. Con el término de la configuración en los equipos se logrará cumplir con el procedimiento de la comunicación de forma eficiente y automática por el mejor camino basado en rutas.

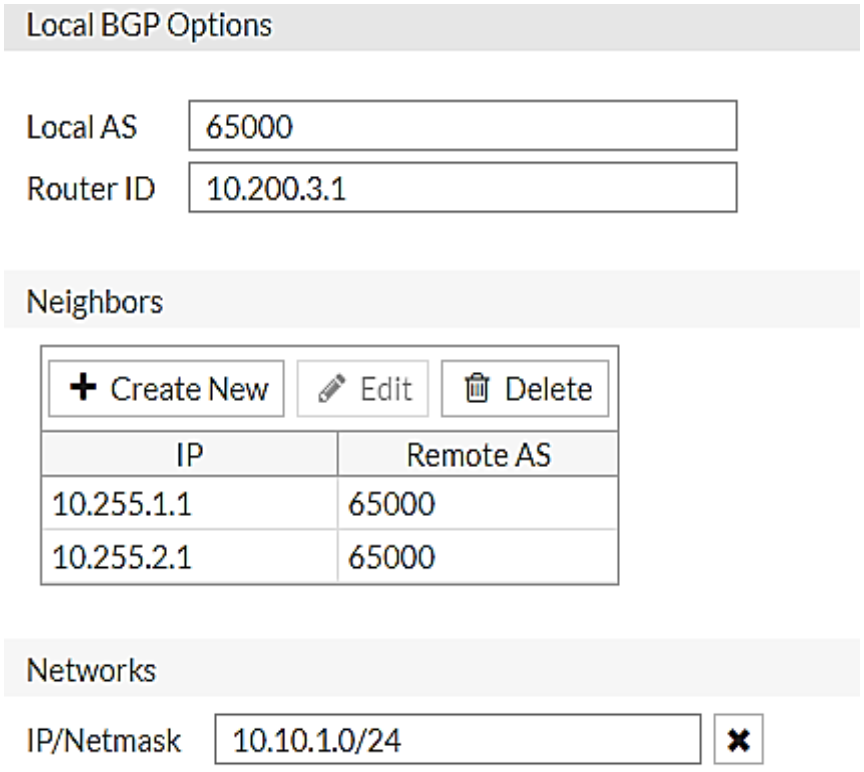


Figura 58. Configuración de BGP de la Tienda 1

Fuente: (Elaboración Propia, 2020)

4.2.4.8. Configuración de SD-WAN.

Llegamos a la parte fundamental de las configuraciones donde se definirá el esquema de balanceo por medio de los algoritmos inteligentes para la distribución y clasificación de las redes para la implementación de un rendimiento óptimo de la red LAN para lograr la optimización de la comunicación de la transmisión de datos. La primera parte se habilitará el SD-WAN para la Oficina Central lo cual usará un balanceo de 1 a 1, lo cual se aprovechará los dos enlaces dedicados para responder las solicitudes de los usuarios de las Tiendas.

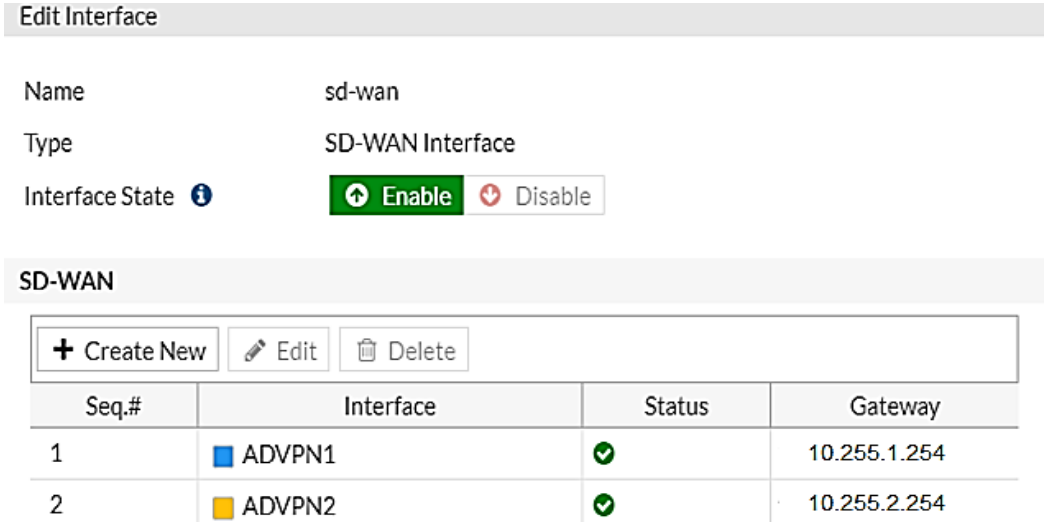


Figura 59. Configuración de SD-WAN de la Oficina Central

Fuente: (Elaboración Propia, 2020)

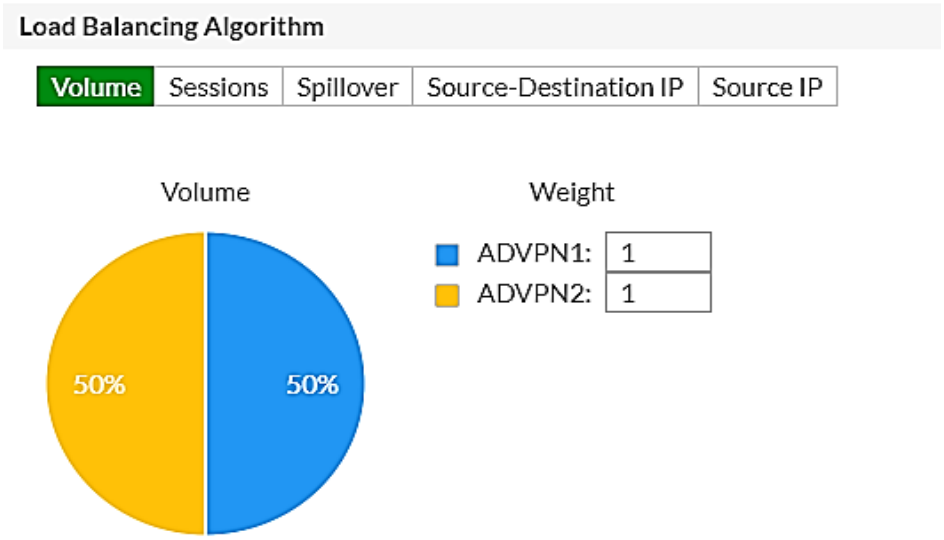


Figura 60. Configuración del Mecanismo de balanceo de la Oficina Central

Fuente: (Elaboración Propia, 2020)

El alcance de la siguiente configuración de IP SLA, se construirá el sensor por tiempo de respuesta hacia un destino público para él envió del tráfico de manera automática a través del mejor canal de enlace donde se tiene la menor latencia para el mejor uso de la comunicación de datos.

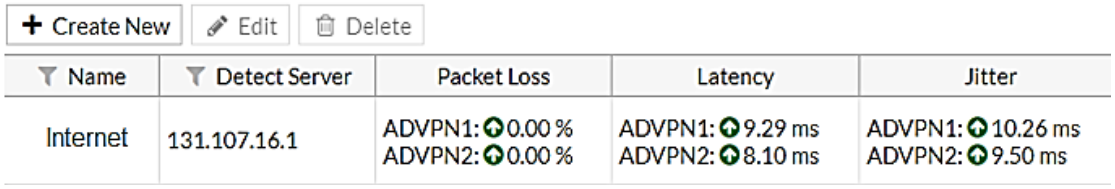


Figura 61. Configuración del Mecanismo de IP SLA Oficina Central

Fuente: (Elaboración Propia, 2020)

Para las configuraciones de SD-WAN de las tiendas se usará el mecanismo basado en rutas para clasificar y forzar el tráfico para enviar las comunicaciones prioritarias y no prioritarias para la distribución de los usuarios para el mejor uso del canal de ancho de banda de las sucursales.

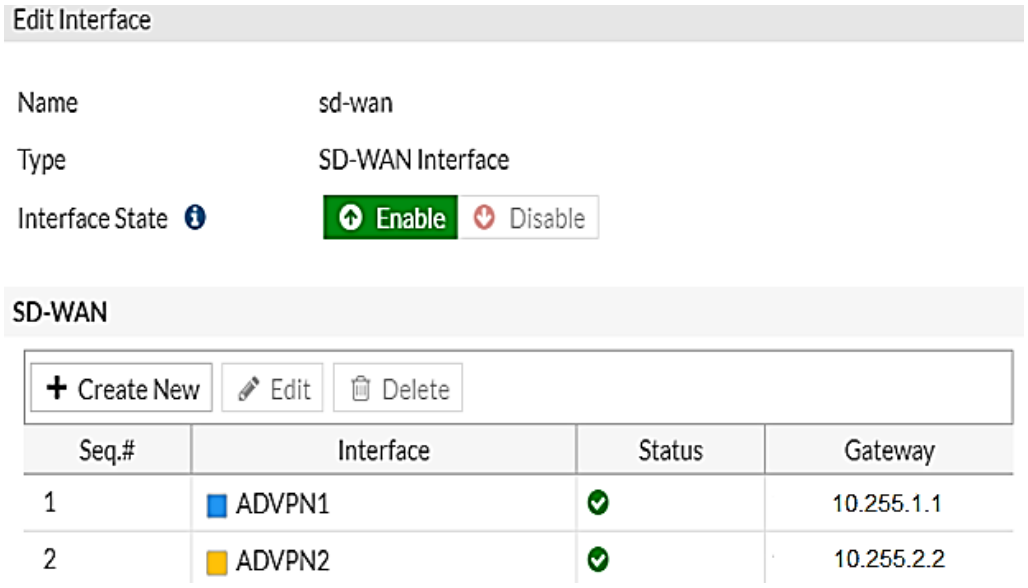


Figura 62. Configuración de SD-WAN Tienda 1

Fuente: (Elaboración Propia, 2020)

Para de definir la clasificación de las redes prioritaria y no prioritarias se dará por la opción de reglas de SD-WAN, con esta funcionalidad se obtendrá el mejor rendimiento de los usuarios clasificando la comunicación de los cajeros por el enlace prioritario de L2L como los usuarios no prioritarios que se manejará la comunicación por medio del enlace de la red 4G. Las reglas se tomarán por el orden de forma descendente. Es decir, las políticas se deberán definir de las más específicas a la más generales.

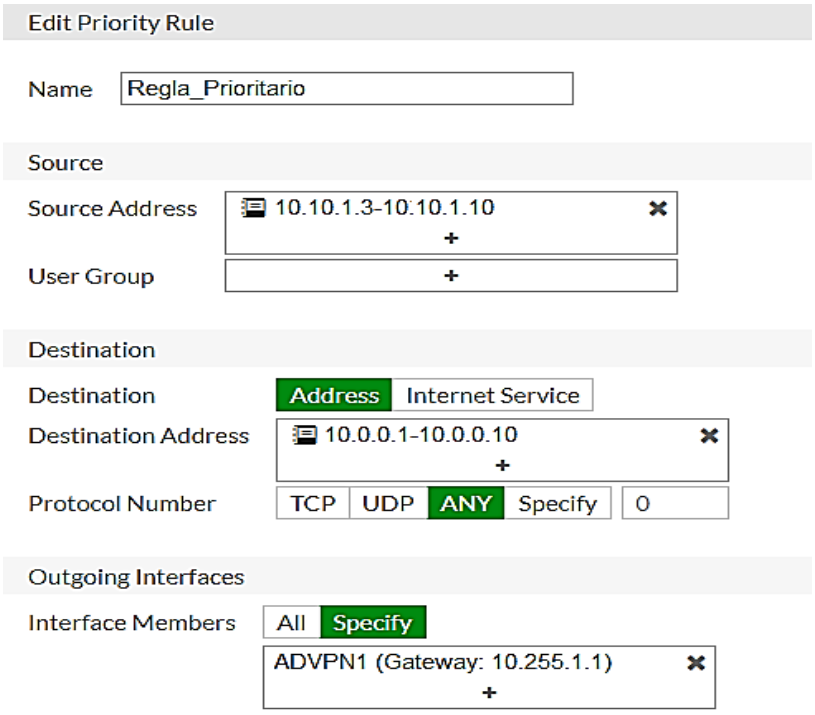


Figura 63. Configuración de la Regla Prioritaria Tienda 1

Fuente: (Elaboración Propia, 2020)

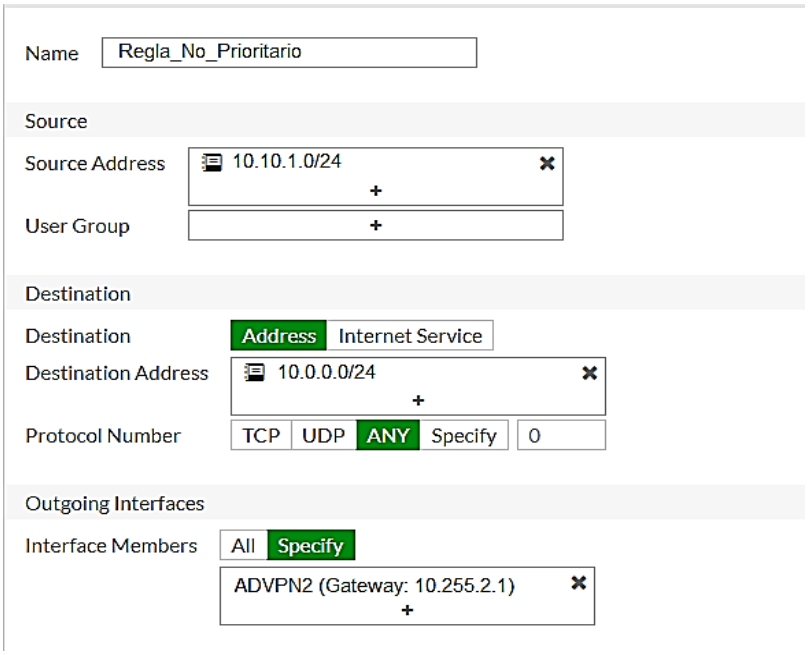
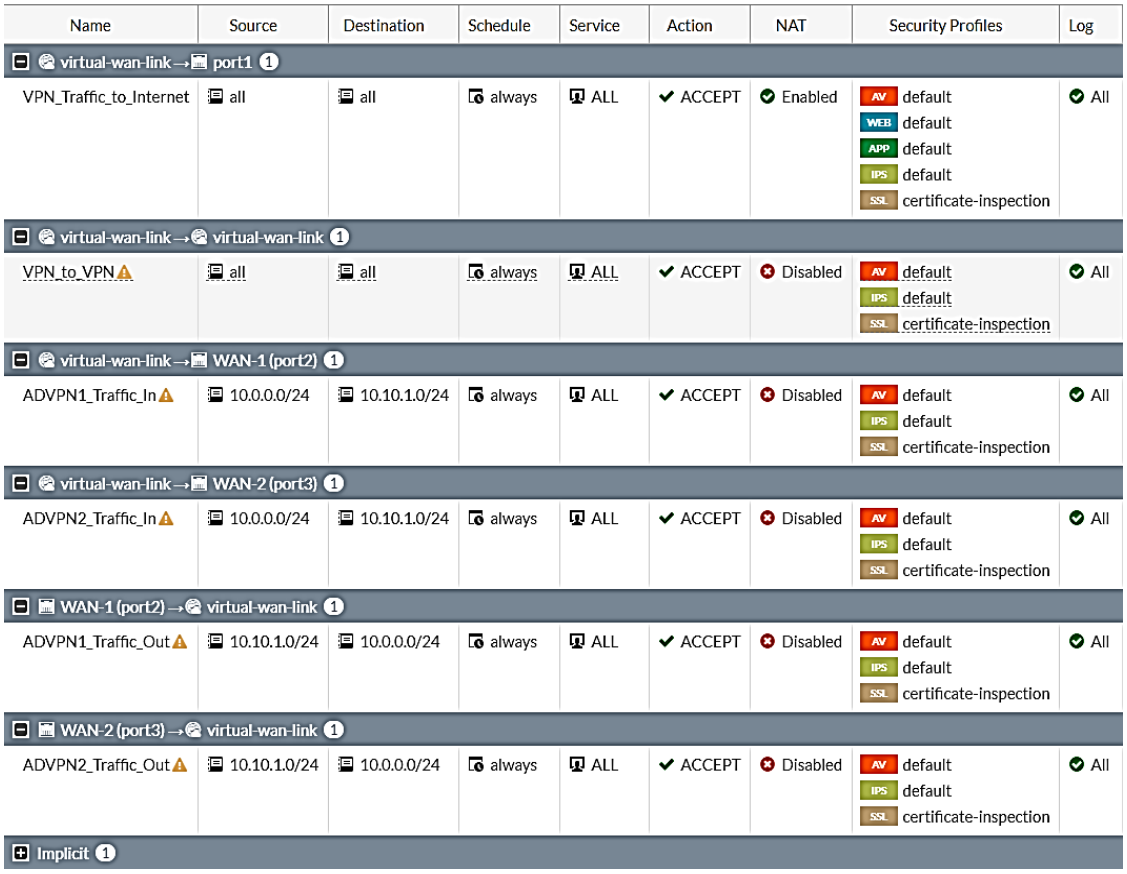


Figura 64. Configuración de la Regla No Prioritario Tienda 1

Fuente: (Elaboración Propia, 2020)

4.2.4.9. Configuración de Políticas.

La parte de la configuración de políticas es sumamente importante ya que a través de ellas se permitirá el tráfico de origen a destino entre las redes WAN y LAN y tenemos que considerar todos lo mecanismo de seguridad para manejar una comunicación efectiva y segura. Así como las reglas de SD-WAN el flujo de acceso es de forma ascendente de arriba hacia abajo.



Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
virtual-wan-link → port1 1								
VPN_Traffic_to_Internet	all	all	always	ALL	ACCEPT	Enabled	AV default WEB default APP default IPS default SSL certificate-inspection	All
virtual-wan-link → virtual-wan-link 1								
VPN_to_VPN	all	all	always	ALL	ACCEPT	Disabled	AV default IPS default SSL certificate-inspection	All
virtual-wan-link → WAN-1 (port2) 1								
ADVPN1_Traffic_In	10.0.0.0/24	10.10.1.0/24	always	ALL	ACCEPT	Disabled	AV default IPS default SSL certificate-inspection	All
virtual-wan-link → WAN-2 (port3) 1								
ADVPN2_Traffic_In	10.0.0.0/24	10.10.1.0/24	always	ALL	ACCEPT	Disabled	AV default IPS default SSL certificate-inspection	All
WAN-1 (port2) → virtual-wan-link 1								
ADVPN1_Traffic_Out	10.10.1.0/24	10.0.0.0/24	always	ALL	ACCEPT	Disabled	AV default IPS default SSL certificate-inspection	All
WAN-2 (port3) → virtual-wan-link 1								
ADVPN2_Traffic_Out	10.10.1.0/24	10.0.0.0/24	always	ALL	ACCEPT	Disabled	AV default IPS default SSL certificate-inspection	All
Implicit 1								

Figura 65. Configuración de Políticas de Comunicación

Fuente: (Elaboración Propia, 2020)

4.2.4.10. Check-list de Configuración.

A continuación, se desplegará el check-list de configuración por medio de líneas de comandos para el registro y documentación de la implementación de Secure SD-WAN.

Interfaces & Routing: Configuración de las interfaces WAN/LAN del Fortigate y Rutas	
config system interface	Interfaz WAN1-L2L
edit "**port1**"	IP de comunicación con ISP1 L2L
set ip **10.200.1.1 255.255.255.0**	
set allowaccess ping https ssh	
set alias "WAN-1"	
next	
edit "**port2**"	Interfaz WAN2-L2L
set ip **10.200.2.1 255.255.255.0**	IP de comunicación con ISP2 L2L
set allowaccess ping https ssh	
set alias "WAN-2"	
next	
edit "**port3**"	Interfaz LAN
set ip **10.0.0.1 255.255.255.0**	IP LAN de la Oficina Central
set allowaccess ping https ssh	
set alias "LAN"	
next	
edit "**wan1**"	Interfaz WAN-Internet
set ip **181.177.224.2 255.255.255.248**	IP WAN Pública
set allowaccess ping https ssh	
set alias "WAN-Internet"	
next	
end	
config router static	Configuración de rutas estáticas
edit 0	Ruta default por la interfaz de acceso a Internet
set dst 0.0.0.0 0.0.0.0	
set gateway **181.177.224.2**	
set device "**wan1**"	
next	
edit 0	
set dst **10.200.3.0/24**	Ruta hacia la tienda 1
set gateway **10.200.1.254**	Puerta de Enlace WAN1-L2L
set device "**port1**"	
next	
edit 0	
set dst **10.200.4.0/24**	Ruta hacia la tienda 1
set gateway **10.200.2.254**	Puerta de Enlace WAN2-L2L
set device "**port2**"	
next	
end	

ADVPN IPsec: Configuración de ADVPN en la Oficina Central	
config vpn ipsec phase1-interface	Nombre Fase1 de VPN1(DialUp)
edit "ADVPN1"	
set type dynamic	
set interface **"port1"**	Declara origen de VPN1 la WAN1-L2L
set local-gw **10.200.1.1**	Puerto de Enlace Local - IP WAN1-L2L
set peertype any	
set proposal des-sha1	
set add-route disable	
set dpd on-idle	
set dhgrp 2	
set auto-discovery-sender enable	
set net-device enable	
set psksecret **<password>**	Clave pre-compartida de VPN1
set dpd-retryinterval 2	
next	
edit "ADVPN2"	Nombre Fase1 de VPN2 (DialUp)
set type dynamic	
set interface **"port2"**	Declara origen de VPN1 la WAN2-L2L
set local-gw **10.200.2.1**	Puerta de Enlace Local - IP WAN2-L2L
set peertype any	
set proposal des-sha1	
set add-route disable	
set dpd on-idle	
set dhgrp 2	
set auto-discovery-sender enable	
set net-device enable	
set psksecret **<password>**	Clave pre-compartida de VPN2
set dpd-retryinterval 2	
next	
end	
config vpn ipsec phase2-interface	
edit "ADVPN1-P2"	Nombre fase 2 de VPN1 (DialUp)
set phase1name "ADVPN1"	
set proposal des-sha1	
next	
edit "ADVPN2-P2"	Nombre fase 2 de VPN2 (DialUp)
set phase1name "ADVPN2"	
set proposal des-sha1	
next	
end	

VPN Interfaz: Asignación de direccionamiento a las interfaces VPN.	
config system interface	
edit "ADVPN1"	Nombre de Interfaz VPN1
set ip **10.255.1.1 255.255.255.255**	IP Local de la interfaz VPN1
set allowaccess ping	Habilitar respuesta de icmp
set type tunnel	
set remote-ip **10.255.1.2 255.255.255.255**	IP Remota de la interfaz VPN1
set interface "port1"	
next	
edit "ADVPN2"	Nombre de Interfaz VPN2
set ip **10.255.2.1 255.255.255.255**	IP Local de la interfaz VPN2
set allowaccess ping	Habilitar respuesta de icmp
set type tunnel	
set remote-ip **10.255.2.2 255.255.255.255**	IP Remota de la interfaz VPN2
set interface "port2"	
next	
end	

Prefix List & Route Map: Objetos para aplicar el control de rutas dinámicas.	
config router prefix-list	
edit "PL_DEFAULT"	Prefix List que hace match con la ruta default
config rule	
edit 1	
set prefix 0.0.0.0 0.0.0.0	Prefijo de coincidencia.
unset ge	
unset le	
next	
end	
next	
end	
config router route-map	Route-Map para match con la ruta default con la BGP.
edit "RM_DEFAULT"	
config rule	
edit 1	
set match-ip-address "PL_DEFAULT"	Prefix list de coincidencia.
next	
end	
next	
end	

Configuración de BGP: Se aplica el enrutamiento dinámico con los vecinos	
config router bgp	Configuración BGP
set as 65000	AS Local
set router-id **10.0.0.1**	ID Local (IP LAN)
set keepalive-timer 1	Reducción de timers BGP
set holdtime-timer 3	
set ibgp-multipath enable	Habilitar múltiples rutas en un iBGP
set scan-time 5	
config neighbor-group	
edit "ADVPN1-PEERS"	Configuración de vecinos peer-group VPN1
set advertisement-interval 1	
set capability-default-originate enable	Anuncio de la ruta default
set link-down-failover enable	
set next-hop-self enable	
set soft-reconfiguration enable	
set default-originate-routemap "RM_DEFAULT"	Anuncio default condicional con route-map
set remote-as 65000	AS Remoto (iBGP)
set route-map-out "RM_DEFAULT"	Filtro de anuncio out en BGP
set route-reflector-client enable	Función de route-reflector en el iBGP.
next	
edit "ADVPN2-PEERS"	Configuración de vecinos peer-group VPN2
set advertisement-interval 1	
set capability-default-originate enable	Anuncio default
set link-down-failover enable	
set next-hop-self enable	
set soft-reconfiguration enable	
set default-originate-routemap "RM_DEFAULT"	Anuncio default condicional con route-map
set remote-as 65000	AS Remoto (iBGP)
set route-map-out "RM_DEFAULT"	Filtro de anuncio out en BGP
set route-reflector-client enable	Función de route-reflector en el iBGP.
next	
end	
config neighbor-range	Config neighbor-range
edit 1	
set prefix 10.255.1.0 255.255.255.0	Pool IP’s de neighbors en la VPN1
set neighbor-group "ADVPN1-PEERS"	Asociarlos al neighbor-group de VPN1
next	
edit 2	
set prefix 10.255.2.0 255.255.255.0	Pool IP’s de neighbors en la VPN2
set neighbor-group "ADVPN2-PEERS"	Asociarlos al neighbor-group de VPN2
next	
end	
end	

SD-WAN: Se declaran las interfaces que se integran a la interfaz virtual de balanceo.	
config system sdwan	
set status enable	Habilita la interfaz SDWAN
set load-balance-mode measured-volume-based	Algoritmo default de balanceo (peso)
config members	
edit 1	
set interface **"ADVPN1"**	Interfaz de balanceo 1 – VPN1
set volume-ratio **1**	Volumen de balanceo 1
next	
edit 2	
set interface **"ADVPN2"**	Interfaz de balanceo 2 – VPN2
set volume-ratio **1**	Volumen de balanceo 1
next	
end	
end	

Políticas: Reglas para permitir el tráfico In/Out por las interfaces SD-WAN	
config firewall policy	
edit 0	Crea nueva política
set name "VPN_Traffic_Out"	Nombre: Permite tráfico VPN saliente
set srcintf **"port3"**	Interface Origen: LAN
set dstintf "virtual-wan-link"	Interface Destino: SD-WAN
set srcaddr "all"	
set dstaddr "all"	
set action accept	
set schedule "always"	
set service "ALL"	
set logtraffic all	
next	Crea nueva política
edit 0	Nombre: Permite tráfico VPN entrante
set name "VPN_Traffic_In"	Interface Origen: SD-WAN
set srcintf "virtual-wan-link"	Interface Destino: LAN
set dstintf **"port3"**	
set srcaddr "all"	
set dstaddr "all"	
set action accept	
set schedule "always"	
set service "ALL"	
set logtraffic all	
next	
edit 0	Crea nueva política
set name "VPN_to_VPN"	Nombre: Permite tráfico entre SD-WAN
set srcintf "virtual-wan-link"	Interface Origen: SD-WAN
set dstintf "virtual-wan-link"	Interface Destino: SD-WAN
set srcaddr "all"	
set dstaddr "all"	
set action accept	
set schedule "always"	
set service "ALL"	
set logtraffic all	
next	

edit 0 set name "VPN_Traffic_to_Internet" set srcintf "virtual-wan-link" set dstintf "WAN-Internet" set srcaddr "all" set dstaddr "all" set action accept set schedule "always" set service "ALL" set logtraffic all set nat enable next end	Crea nueva política Nombre: Permite tráfico de las VPN a Internet Interface Origen: SD-WAN Interface Destino: Interfaz de Internet

4.2.4.11. Comprobación de funcionamiento de la simulación.

A continuación, se describe el procedimiento para verificar las configuraciones aplicadas tanto para la Agencia Principal como para la tienda 1. Con la finalidad de corroborar cada detalle de la implementación del protocolo Secure SD-WAN para garantizar el buen funcionamiento del servicio. Asimismo, ayudará para resolver cualquier incidencia.

4.2.4.11.1. Estado de las configuraciones aplicadas.

La comprobación de los estados de configuraciones se llevará a cabo mediante el acceso al equipo Fortigate en sus diferentes niveles de plataforma a través del entorno gráfico (GUI) o el entorno de consola (CLI).

- **Revisión del Túnel VPN Ipsec:** Esta función es útil para validar el estado de conexión de los túneles ADVPN, se puede acceder desde la función de Monitor del equipo en la interfaz gráfica y validar el estado de la sesión, si se encuentra Activo o caído. Para el correcto funcionado el estado de la conexión deberá estar en UP.

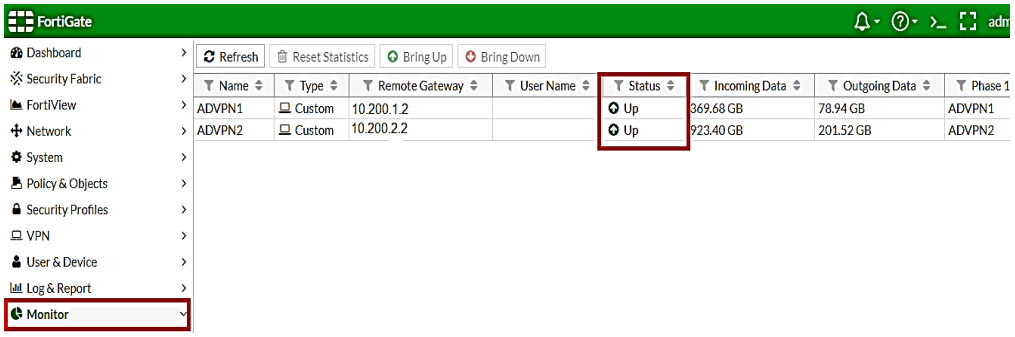


Figura 66. Estado de Conexión de la ADVPN

Fuente: (Elaboración Propia, 2020)

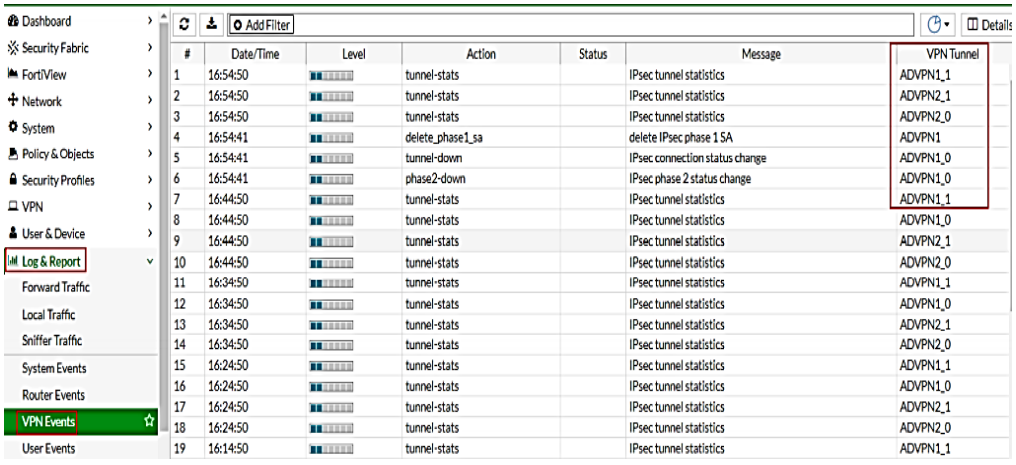


Figura 67. Log de sincronización de la ADVPN

Fuente: (Elaboración Propia, 2020)

- **Revisión de BGP:** La revisión se efectuará por la consola de CLI por la línea de comando get router info bgo sumary, se informará el estado de la sesión BGP y el tiempo que está establecido.

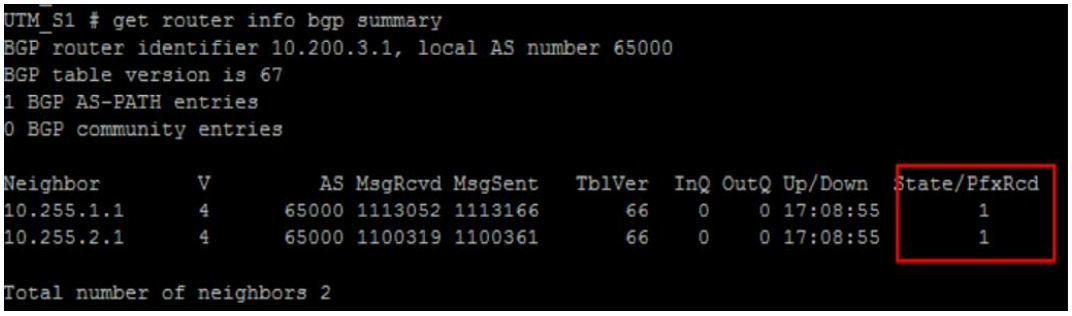


Figura 68. Estado de la Sesión de BGP

Fuente: (Elaboración Propia, 2020)

La siguiente imagen muestra la tabla de enrutamiento BGP por la línea de CLI get router info routing-table all.

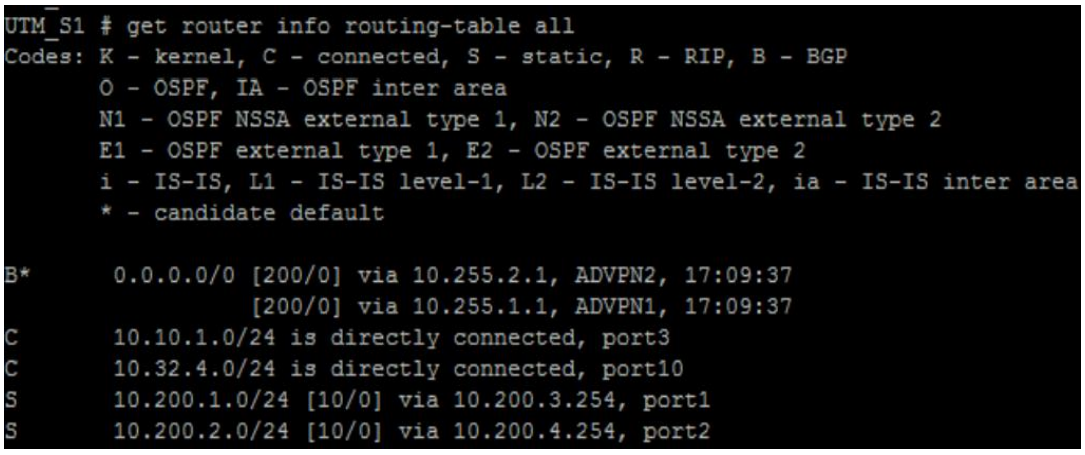


Figura 69. Tabla de Enrutamiento de Vecindad BGP

Fuente: (Elaboración Propia, 2020)

- **Revisión de SD-WAN:** Para revisar el estado de salud SD-WAN se accederá por el entorno gráfico del equipo donde se visualizará la medición del tiempo de respuesta monitoreado por los mecanismos de balanceo inteligentes, esta parte es importante para controlar y monitorear la configuración de SD-WAN.

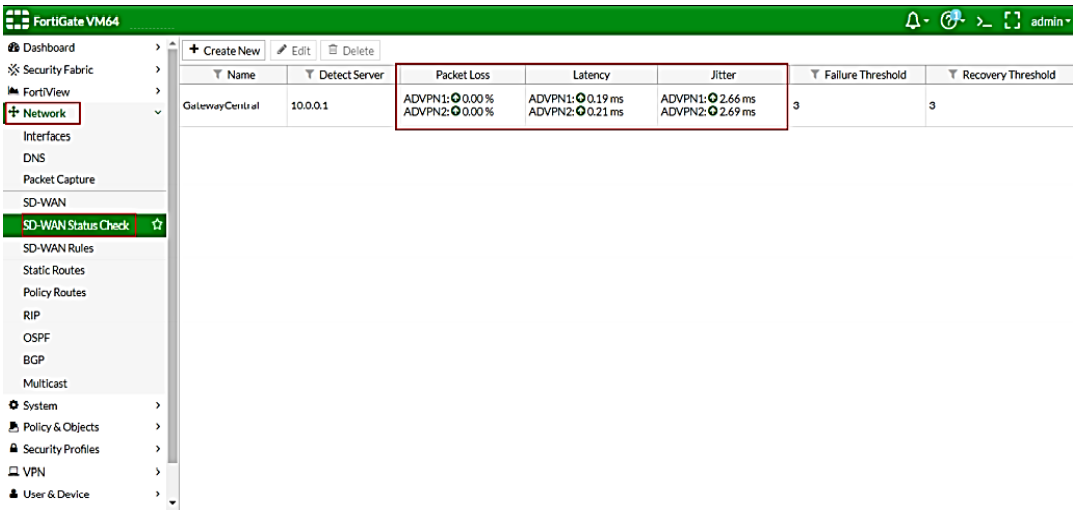


Figura 70. Estado de Salud de los sensores de SD-WAN

Fuente: (Elaboración Propia, 2020)

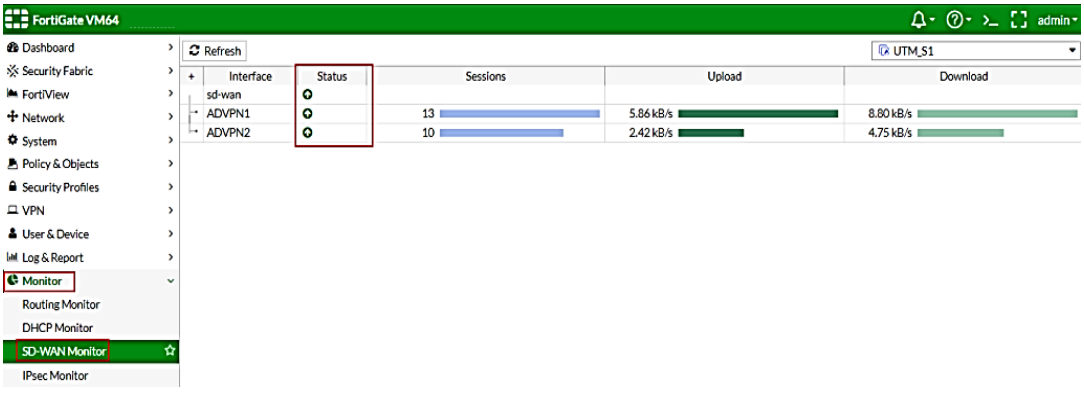


Figura 71. Monitor de Estado de SD-WAN

Fuente: (Elaboración Propia, 2020)

4.2.5. Etapa 5 Operación

4.2.5.1. Procedimiento de monitoreo.

La solución implementada considera el acoplamiento de monitoreo mediante el uso de recopilación de datos por el protocolo SNMP. Se ha contemplado así las configuraciones requeridas en las diferentes herramientas de la empresa como los sistemas de PRTG, CACTI. El área de monitoreo y centro de atención al cliente ha definido las siguientes consideraciones para el monitoreo a realizarse de los equipamientos que confirma la solución de Secure SD-WAN:

- Alerta de los equipamientos mediante la herramienta de PRTG.
- Monitoreo del consumo de ancho de banda y calidad de enlace mediante la herramienta CACTI.
- Registro de Actividades que se llevará a cabo mediante una plataforma web.

En esta etapa, se acordó realizar un seguimiento permanente dentro de los horarios establecidos por Cencosud S.A. El monitoreo a incidencias será validado directamente por el área de redes y comunicaciones. Para el registro de los eventos que involucre la indisponibilidad de cualquier funcionalidad contemplada dentro de la solución del Secure SD-WAN, será analizado y registrado dentro de una Bitácora de Hechos Relevantes.

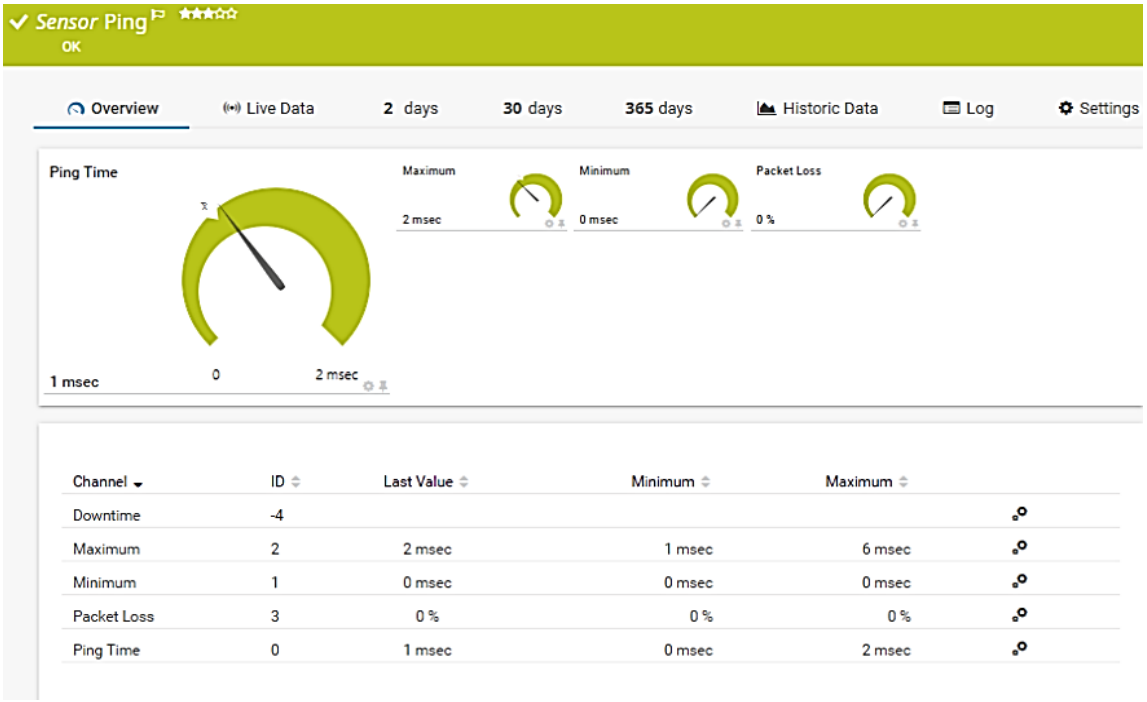


Figura 72. Monitoreo de sensor ICMP, herramienta PRTG

Fuente: (PAESSLER, 2020)

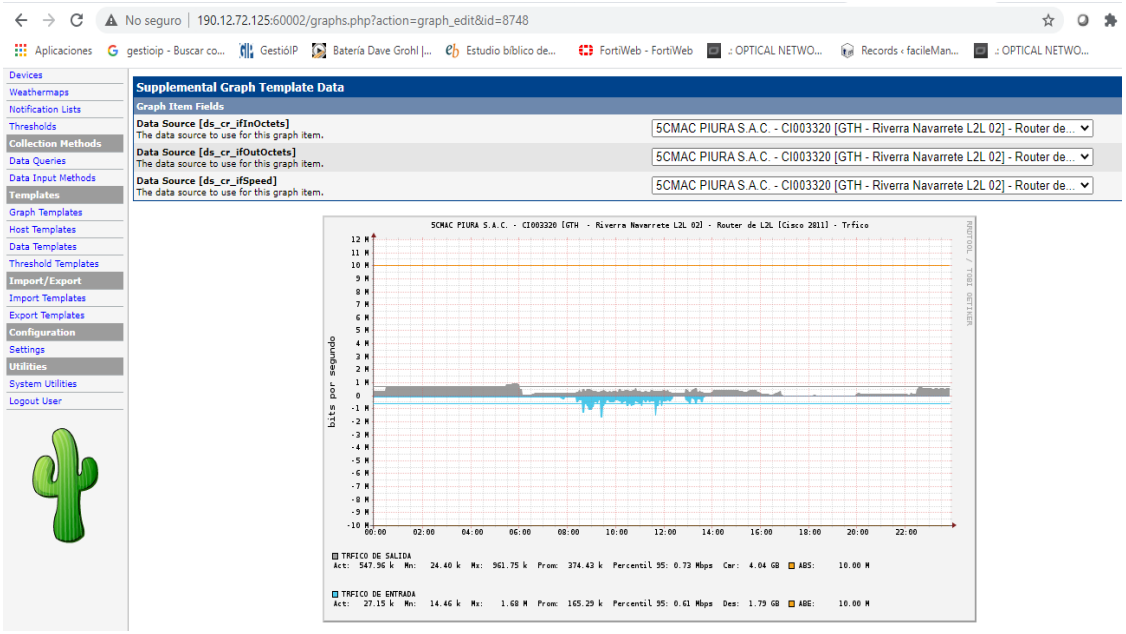


Figura 73. Monitoreo de ancho de banda, herramienta CACTI

Fuente: (Elaboración Propia, 2020)

4.2.5.2. Procedimiento de registro en la bitácora de hechos relevantes.

Con referencia al procedimiento de registro de la BHR, se ha elaborado el siguiente procedimiento que involucra a las áreas que participarán en el procedimiento para el cumplimiento de la tarea propuesta en la etapa de operación. El formato de la BHR esta detallado en el Anexo 2 “Formato de bitácora de hechos relevantes”.

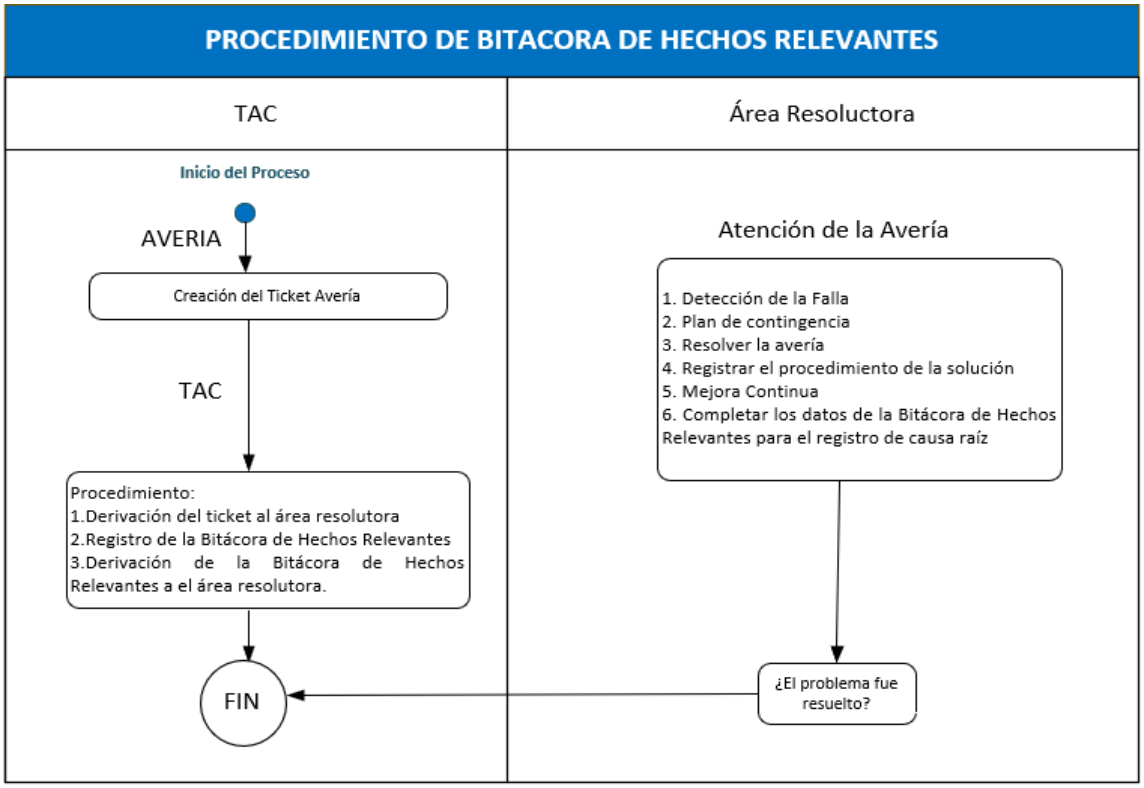


Figura 74. Flujograma del procedimiento de la BHR

Fuente: (Elaboración Propia, 2020)

4.2.5.3. Actividades del mantenimiento preventivo.

El servicio de mantenimiento preventivo se deberá realizar en un periodo trimestral, lo cual se verificará el estado y el rendimiento del equipamiento que participan en la solución de Secure SD-WAN, las tareas a realizar serían las siguientes y será encargado en conjuntos por el equipo del área de Telecomunicaciones de la empresa Cencosud con el

proveedor de servicios de los enlaces dedicados, se adjunta el formato de Mantenimiento Preventivo en el Anexo 3 “Formato de mantenimiento preventivo”.

- Servicio de diagnóstico, test y reparación de los equipamientos.
- Limpieza y mantenimiento externo de los equipamientos.
- Limpieza de los componentes ópticos de los enlaces de transmisión de datos.
- Medición de la calidad de los enlaces de fibra óptica.
- Medición de los valores de la alimentación eléctrica de los equipamientos.
- Medición de los niveles de seguridad de los equipamientos.

4.2.5.4. Procedimiento de RMA.

El reemplazo de dispositivos Fortinet que cumple la función de SD-WAN, debido a fallas en el hardware sigue el siguiente procedimiento para que Fortinet haga efectiva el envío del nuevo hardware por avería de equipos.

- **Creación de ticket:** Este paso es la apertura para la inspección del hardware solicitado por el TAC de Fortinet a través de la web de soporte.
- Diagnóstico de las pruebas de HQIP (2 horas): Muestra los resultados positivos (PASS) o negativos (FAILED).
- Tiempo de envío (30 días): El tiempo de envío es de 30 días útiles desde confirmada la reasignación del ticket a RMA
- Recepción de hardware (2 horas): Cumplido los 30 días útiles el hardware es recibido.
- **Entrega de hardware:** Almacén hace efectiva el nuevo hardware al área de comunicaciones para su instalación.

4.2.6. Etapa 6 Optimización

En el desarrollo de esta etapa, se finaliza el periodo de pruebas de la solución Secure SD-WAN, por lo cual se formaliza la entrega del proyecto al área de atención al cliente (TAC) quienes realizarán las siguientes tareas descritas para mantener la red operando de forma continua con la máxima calidad de entrega del servicio a los usuarios de la empresa Cencosud S.A.

- Monitoreo continuo de los enlaces y equipamiento a través de las herramientas de monitoreo.
- Registro de cualquier incidencia en el documento bitácora de hechos relevantes
- Generación de los backups de configuración de forma semanal
- Mantener actualizado el inventario de los equipos
- Actualización de la plantilla de configuración
- Soporte a incidencia para la solución de cualquier impase en el menor tiempo posible para la disminución de cualquier impacto en la producción.
- Solicitud de requerimientos de los usuarios de la red

Debido a lo antes expuesta el encargado del área del TAC avalará las funciones y las tareas asignadas en el documento para el cumplimiento de los estándares para el buen funcionamiento del servicio y se brinde la mejor experiencia de los usuarios de la red para el uso de las aplicaciones de forma rápida, segura, integra y disponible en cualquier momento.

CAPÍTULO V

Instrumentos de Medición

5.1. Indicadores de medición

Para la evaluación de los indicadores se ha definido las siguientes métricas de medición de valor numérico para analizar los resultados de la solución de Secure SD-WAN y evaluar su viabilidad, en la siguiente tabla se mostrará los indicadores de la medición empleado para el proyecto de tesis.

Tabla 8

Indicadores de Medición

Ítem	Indicador	Valor de medida
1	Capacidad de red	Mbps
2	Tiempo de respuesta de los sistemas informáticos	Milisegundos (ms)
3	Experiencia del usuario	Porcentaje (%)

Nota: Métrica de medición. Autoría propia

5.2. Indicadores de cumplimiento

Para medir los resultados de los objetivos definidos en el Capítulo I “Antecedentes del Problema” se realizará una comparación de los valores estadísticos del antes y después de la solución aplicada para que se pueda evaluar su efectividad y los logros de dichos objetivos y el progreso de ello a través de la recopilación de información representados en gráficos estadísticos.

5.2.1. Capacidad de red

Para medir la capacidad de red, se utilizó el valor de medida de Mbps, para determinar el consumo de ancho de banda de las tiendas en un periodo de 11 meses, y evaluar el rendimiento de red en la actualidad de la empresa Cencosud S.A. Para la representación de los valores, se detallará el consumo por gráfico en barras de la Oficina Central y de las tiendas sucursales por separados, la línea roja significa el ancho de banda contratado y el tope de consumo que deberá ocurrir para el uso de los sistemas informáticos. Por otro punto, se representará la capacidad de red posterior al desarrollo de la solución de Secure SD-WAN recopilado en el mes de diciembre del 2020 para la mejora de performance se realizó la división de enlaces para el balaceo del tráfico prioritario y no prioritarios para un mejor control de ancho de banda, lo cual observamos una optimización de los recursos de L2L permitiendo contar con canales libres y reserva de ancho de banda para alguna ampliación dentro de la red interna, así cumpliendo con la optimización de la capacidad de red.

- Gráfico estadístico antes de la solución de Secure SD-WAN

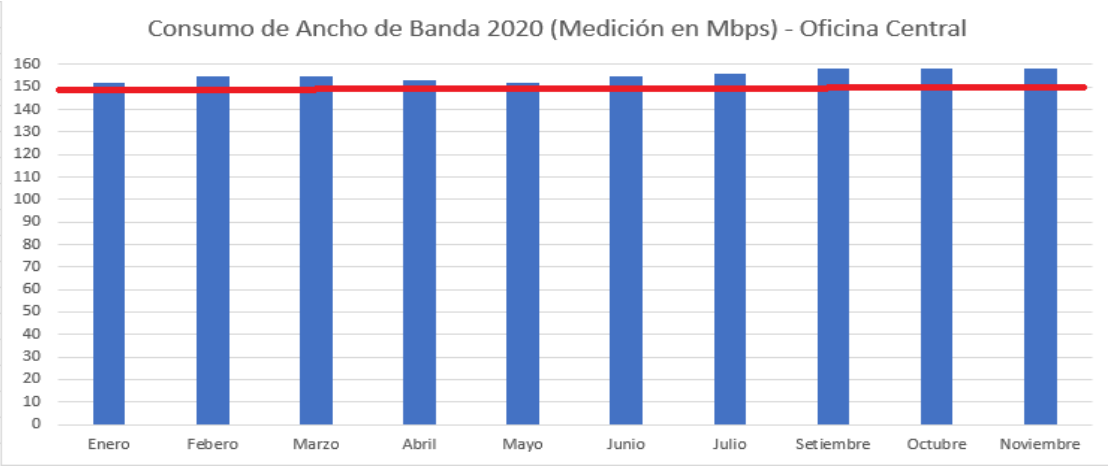


Figura 75. Capacidad de red – Oficina Central – Antes de la solución

Fuente: (Elaboración Propia, 2020)

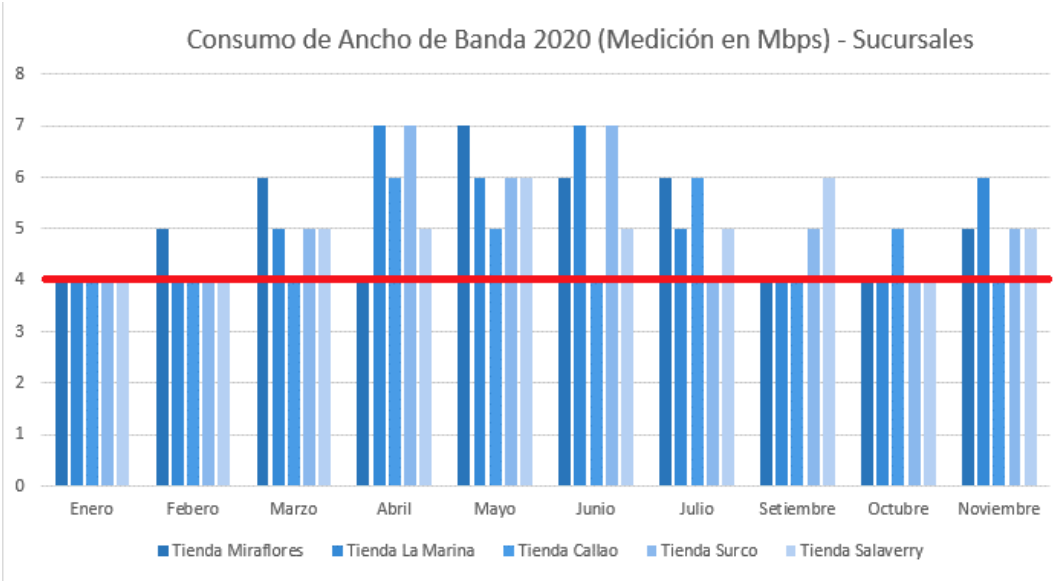


Figura 76. Capacidad de red – Tiendas Sucursales – Antes de la solución

Fuente: (Elaboración Propia, 2020)

- Gráfico estadístico después de la solución de Secure SD-WAN

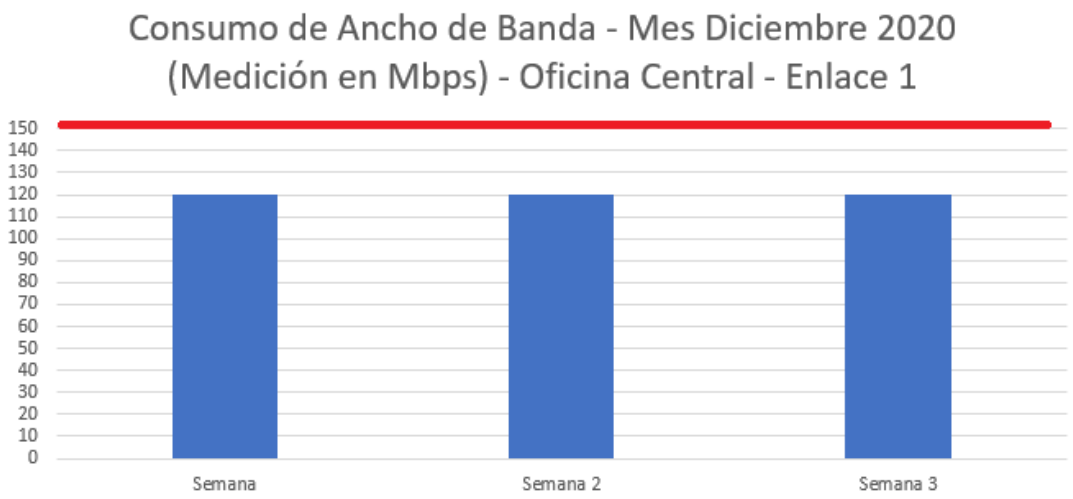


Figura 77. Capacidad de red, Enlace 1 – Oficina Central

Fuente: (Elaboración Propia, 2020)

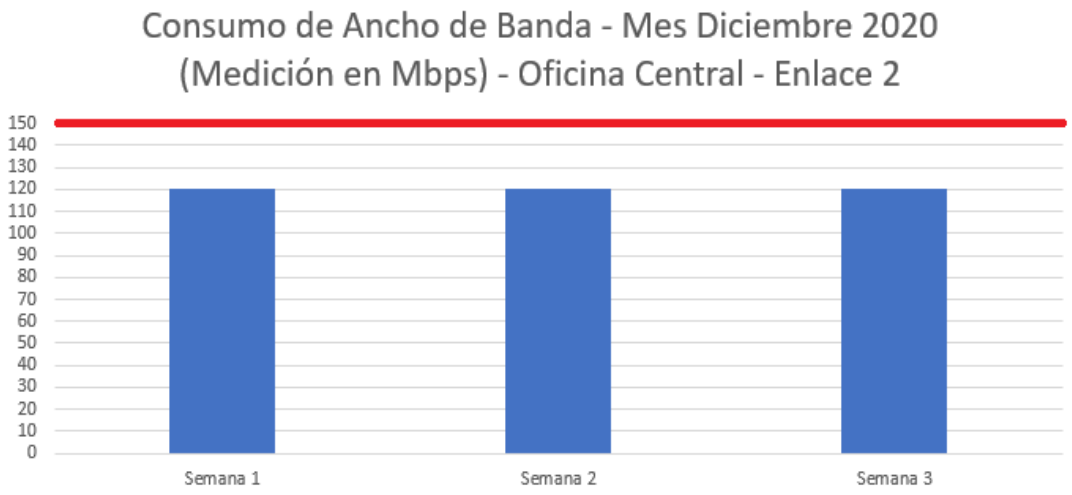


Figura 78. Capacidad de red, Enlace 2 – Oficina Central

Fuente: (Elaboración Propia, 2020)

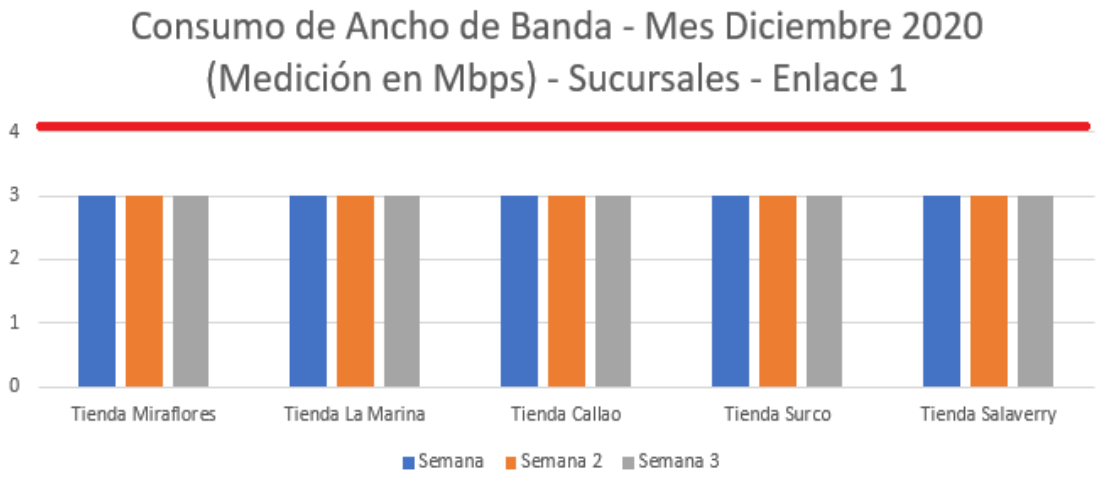


Figura 79. Capacidad de red, Enlace 1 – Tiendas Sucursales

Fuente: (Elaboración Propia, 2020)

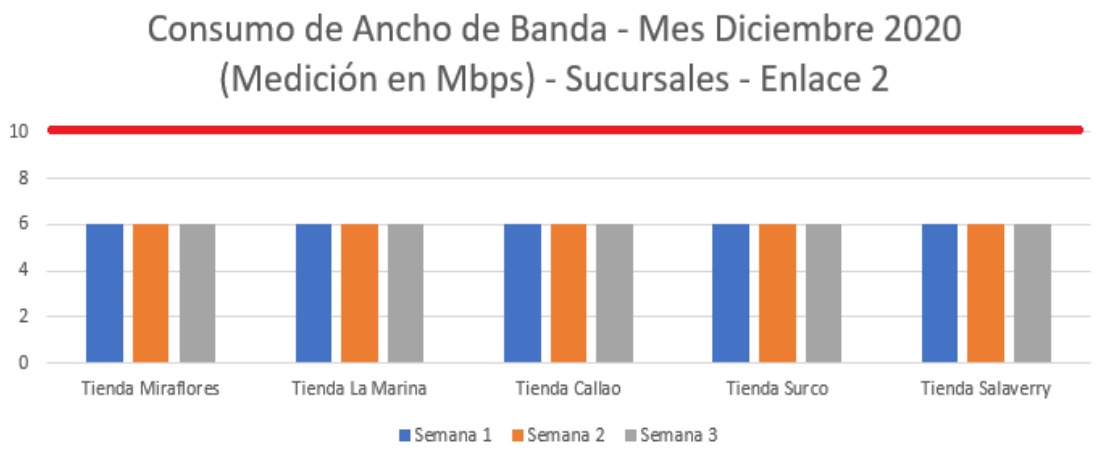


Figura 80. Capacidad de red, Enlace 2 – Tiendas Sucursales

Fuente: (Elaboración Propia, 2020)

5.2.2. Tiempo de respuesta

Para medir el tiempo de respuesta de los sistemas informáticos se utilizó la unidad de valor de milisegundos (ms) para medir la efectividad y accesibilidad de los sistemas informáticos mencionados en el capítulo III Metodología de la investigación, el promedio del tiempo de respuesta debe ser de 0 a 3 ms dentro de la red interna para la mejor interacción del usuario hacia el acceso a los sistemas de la red, lo cual no está ocurriendo actualmente, ya que se registra picos de 6 milisegundos sobrepasando el promedio permitido. Después de la solución aplicada se logró bajar el valor a 1 ms. Así, cumpliendo el estándar dentro del promedio para el mejor desempeño de la red y los usuarios pueda acceder de forma rápida y sin interrupciones.

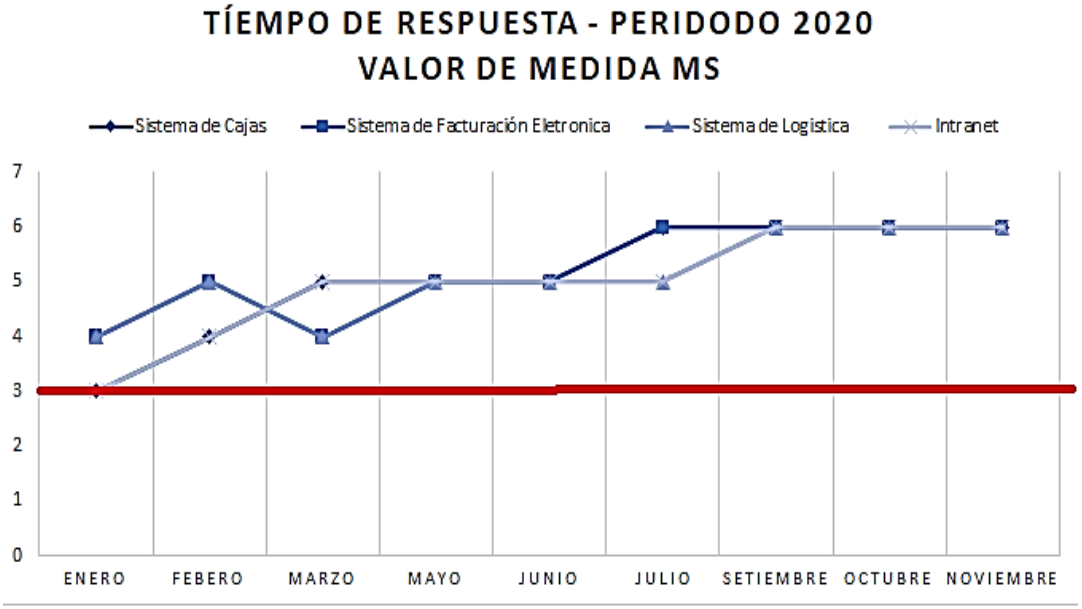


Figura 81. Tiempo de Respuesta de los sistemas informáticos

Antes de la solución

Fuente: (Elaboración Propia, 2020)

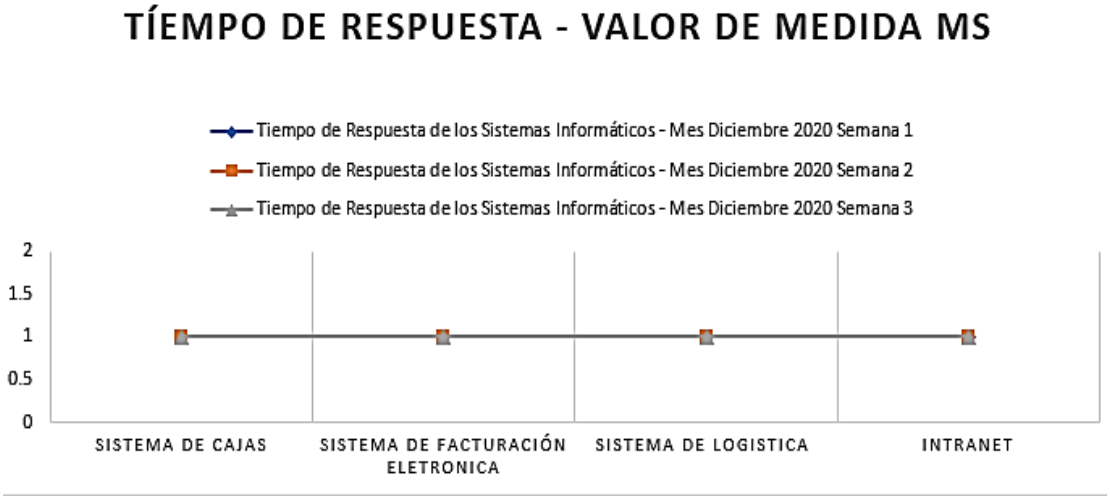


Figura 82. Tiempo de Respuesta de los sistemas informáticos

Después de la solución

Fuente: (Elaboración Propia, 2020)

5.2.3. Encuesta

Se realizó una encuesta a 56 usuarios del área Operativa de Cencosud con la finalidad de validar la solución aplicada de Secure SD-WAN para extraer información valiosa y poder tener conocimiento del rendimiento de la red hora punta de carga de usuarios. Cabe precisar la encuesta está estructurada con 05 preguntas para los usuarios de los sistemas de caja y facturación, la encuesta se mostrará en el Anexo I.

Anexo I: Encuesta Sobre el acceso a los sistemas informáticos y velocidad de red

Objetivo de la Encuesta

Conocer la opinión de los empleados sobre la experiencia en el uso de los sistemas informáticos y la velocidad de la red.

- **Alcance**

  La encuesta se realizó en la provincia de Lima.

- **Tiempo de ejecución**

  La encuesta se realizó en el mes de marzo del año 2021.

- **Diseño Muestral**

  - **Población Objetivo:** Conformada por 56 empleados del área operativa.
  - **Dimensión de la Muestra:** Compuesta por 56 empleados de forma aleatoria.
  - **Trabajo de Campo:** Realizada a los empleados del área operativa.
  - **Procesamiento:** La encuesta fue realizado mediante la herramienta de Google Forms.

- **Número de Preguntas:** 05 distribuidas de la siguiente manera:
    1. ¿En la actualidad trabajan de manera eficiente con los sistemas informáticos?
    2. ¿Presentan problemas de velocidad de red sobre el uso de los sistemas informáticos?
    3. ¿Trabajan de forma ágil y de manera eficiente con la conexión de los sistemas informáticos?
    4. ¿Del 1 al 10 que tan lenta es la conexión con los sistemas informáticos?
    5. ¿Qué quisiera usted que se mejore en el acceso a la red y a los sistemas informáticos?

5.3. Resultados

- **Recopilación de datos:** El primer objetivo fue toda la recopilación de datos que fue usado en los indicadores de cumplimientos, basándonos en la fuente de monitoreo a través de las herramientas de PRTG y Cacti. Lo cual, se logró generar gráficos estadísticos la obtener la métrica de las mediciones de los indicadores propuestos para medir el resultado final de la solución Secure-SDWAN.
- **Capacidad de red:** A parir de los gráficos estadísticos obtenidos, se determinó como influye la capacidad de balanceo de carga a través de la solución de Secure SD-WAN dividendo y clasificando el tráfico de datos, logrando así, controlar y optimizar los recursos de red de forma segura e

inteligente, mostrada en los indicadores de cumplimientos en los puntos de capacidad de red y tiempo de respuesta. Se mejoró un 98.2 % de la confiabilidad y calidad de la red sobre la accesibilidad a los sistemas informáticos como la disminución del porcentaje de los problemas de lentitud en la red, los resultados fueron reflejados en el siguiente cuadro donde se realiza una comparativa del antes y después de la solución SD-WAN.

Resultados	Antes Sin la Solución Respuestas de Usuarios (%)	Después Con la solución Respuestas de Usuarios (%)
Confiabilidad del uso de la red	10%	98.2%
Problemas de lentitud de la red	100%	1%
Eficiencia en la red	4%	98.2%

Figura 83. Cuadro de Resultados de la Encuesta

Fuente: (Elaboración Propia, 2020)

En el cuadro adjunto de los resultados de la encuesta, se formuló una serie de preguntas con la finalidad de comparar las respuestas de los usuarios del área operativa para obtener una estadística del antes y después del desarrollo de la solución “Diseño del Protocolo Secure SD-WAN” y poder registrar los resultados y cuantificar la mejora en el acceso a la red y a los sistemas informáticos, lo valores del cuadro fueron extraídos de las

preguntas formuladas en el Anexo 1 “Encuesta Sobre el acceso a los sistemas informáticos y velocidad de red”

- **Monitoreo:** Para finalizar se tiene un control continuo del monitoreo de los tiempos de respuesta y consumo del ancho de banda mediante las herramientas de PRTG y CACTI para determinar cualquier variación que pueda ocurrir en el futuro.

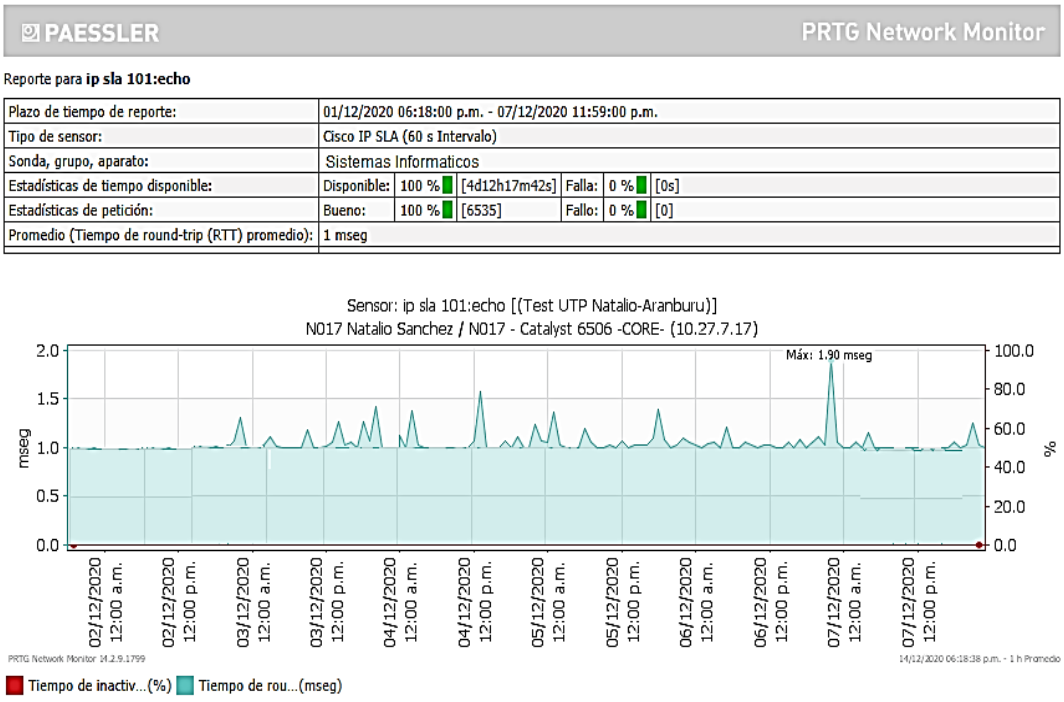


Figura 84. Monitoreo de tiempo de respuesta de los sistemas informáticos

Fuente: (Elaboración Propia, 2020)

CAPÍTULO VI

Análisis Costo Beneficio

6.1. Análisis de costos

En este capítulo se realizará un presupuesto con los elementos necesarios para conformar la propuesta del diseño de protocolo de Secure SD-WAN para el balanceo de enlaces en la empresa Cencosud S.A". Los precios de los elementos de hardware y software varían de acuerdo con los equipos, protocolos y el diseño de red que puedan soportar lo requerido en la solución. Cabe resaltar que todos los recursos fueron elegidos de acuerdo con los parámetros considerados en el proyecto de tesis. Para el presento proyecto se cuenta con inversión Inicial de **S/. 350,000.00** en un tiempo promedio de duración de **6 meses**.

6.1.1. Costos Directos

COSTOS DE PERSONAL (en S/.)				
CARGO	**CANTIDAD**	**COSTO MES**	**MESES**	**COSTO /6 MESES**
Gestor del Proyecto	1	S/.12,000.00	6	S/.72,000.00
Ingeniero de Instalación	1	S/.8,000.00	6	S/.48,000.00
Analista de Instalación	2	S/.7,000.00	6	S/.42,000.00
TOTAL, COSTO DE PERSONAL		**S/.27,000.00**		**S/. 162,000.00**

COSTOS DE RECURSOS MATERIALES				
RECURSOS MATERIALES PARA EL PROYECTO		**CANTIDAD**	**PRECIO UNITARIO**	**TOTAL**
Software (Herramienta)	GNS3	1	S/.0.00	S/.0.00
	VMWARE	1	S/.150.00	S/.150.00
	PRTG	1	S/.400.00	S/.400.00
	CACTI	1	S/.0.00	S/.0.00
Hardware (Equipos)	Fortigate 100E	2	S/. 5,000.00	S/.10,000.00
	Fortigate 50E	89	S/.800.00	S/. 71,200.00
	USB Módem Huawei Modelo E8372	89	S./ 100.00	S/. 8,900.00
TOTAL, COSTOS DE RECURSOS MATERIALES				**S/.90,650.00**

TOTAL, COSTOS DIRECTOS = COSTO DE PERSONAL + COSTOS DE MATERIALES	**S/. 252,650.00**

6.1.2. Costos Indirectos

CAPACITACIONES AL PERSONAL DEL AREA DE TI				
ACTIVIDAD	**CANTIDAD**	**COSTO MES**	**MESES**	**TOTAL**
Capacitación de Secure SD-WAN	5	S/.800.00	1	S/. 4,000.00
Capacitación de Firewall Fortigate	5	S/.800.00	1	S/. 4,000.00
Capacitación de PRTG	5	S/.200.00	1	S/.1,000.00
Capacitación de Cacti	5	S/.160.00	1	S/.800.00
TOTAL, COSTO DE CAPACITACIONES				**S/.9,800.00**

TOTAL, COSTOS INDIRECTOS = COSTOS DE CAPACITACIONES DEL AREA DE TI	**S/.9,800.00**

6.1.3. Costos Fijos

COSTOS DE SERVICIOS (en S/.)			
SERVICIO	**CANTIDAD**	**COSTO / UNIDAD**	**TOTAL**
Costo de Electricidad	1	S/. 160.00	S/. 260.00
Costo de viáticos	3	S/. 30.00	S/. 30.00
Costo de Internet 10 Mbps 4G Entel	89	S/. 70.00	S/. 70.00
TOTAL, DE COSTO FIJOS			**S/. 360.00**

6.1.4. Costos Variables

COSTOS DE ASESORIA (CONSULTORES) (en S/.)				
CARGO	**CANTIDAD**	**COSTO MES**	**MESES**	**COSTO /6 MESES**
Ingeniero Especialista	1	S/.8,000.00	6	S/.48,000.00
Costo de Soporte	1	S/. 3,000.00	6	S/. 18,000.00
TOTAL, COSTO DE PERSONAL		**S/.9,000.00**		**S/. 66,000.00**

TOTAL, COSTOS = COSTOS DIRECTOS + COSTOS INDIRECTOS + COSTOS FIJOS + COSTOS VARIABLES	**S/. 328,810.00**

6.2. Análisis de beneficio

En el siguiente punto se analizará los beneficios tangibles e intangible del protocolo Secure SD-WAN. Asimismo, se mostrará mediante una tabla, la investigación que se realizó en el mercado sobre los 3 fabricantes mejor posicionados en el cuadrante de Gartner para la elección del equipo para la mejor toma de decisión y las necesidades que busca la empresa con respecto a la integridad y seguridad de datos. Con respecto a la información recopilada y por la opción de un mejor precio en el mercado y las funciones requeridas por la empresa, se realizó la elección del fabricante Fortinet para la implementación de la solución.

PROTOCOLO SECURE SD-WAN						
TIPO DE INDICADOR	**DIMENSIONES**	**UNID.**	**FORMULA**	**BENEFICIO**	**MEJORA**	**UNID.**
Intangible	Carga	Kbps	volumen de tráfico medido en Kbps	Incremento en el uso del ancho de banda	Control de ancho de banda	Positivo
	Latencia	Ms	Valor de latencia medido en ms	Buena experiencia del usuario con los accesos a los sistemas informáticos	Rapidez en el acceso a los sistemas informáticos	
Tangible	Avería	%	Porcentaje de N° de averías	Ahorro de costo por Avería	Reducción del impacto en la Red	Positivo
	Rendimiento	%	Porcentaje de enlaces adquiridos	Ahorro en el ancho de banda	Escalabilidad del tráfico en la red	

CUADRO COMPARATIVO SOBRE LAS FUNCIONES DE LOS EQUIPOS SD-WAN				
ÍTEM	**CARACTERISTICA**	**FORTINET**	**PALO ALTO**	**CISCO**
1	Función de SD-WAN	SI	SI	SI
2	Enrutamiento dinámico	SI	SI	SI
3	Túneles ADVPN	SI	SI	SI
4	Seguridad	SI	SI	NO
5	SLA inteligente	SI	SI	SI

CUADRO COMPARATIVO DE LA RELACIÓN DE PRECIO EN EL MERCADO			
ÍTEM	**FABRICANTE**	**MODELO DE EQUIPO**	**COSTO / UNIDAD**
1	Fortinet	50E	S/.800.00
		100E	S/. 5,200.00
2	Palo Alto	PA-220	S/.2,000.00
		PA-820	S/.8,000.00
3	Cisco	ISR-1000	S/. 2,800.00
		ISR-4000	S/.8,300.00

6.3. Análisis de sensibilidad

En esta sección se contemplará los matices del análisis de costo como los flujos de ingresos, flujos de egresos, flujo efectivo neto. Para este proyecto se contempla los resultados en un periodo de 6 meses con valores aproximados, mostrando flujos de ingresos y egresos para con ello poder calcular los flujos efectivo neto que saldría mediante la siguiente formula; **Flujo Efectivo Neto = (flujo de ingresos – flujos de egresos).** Como punto referencial se detalla la inversión inicial **S/. 350,000.00 mil nuevo soles**.

INVERSIÓN INICIAL	S/.350,000.00

FLUJO DE INGRESOS	
	A
Anual	**Valor (en S/.)**
Mes 1	S/.100,450.00
Mes 2	S/.124,500.00
Mes 3	S/.135,000.00
Mes 4	S/.150,103.00
Mes 5	S/.158,459.00
Mes 6	S/.168,459.00
TOTAL	**S/.836,971.00**

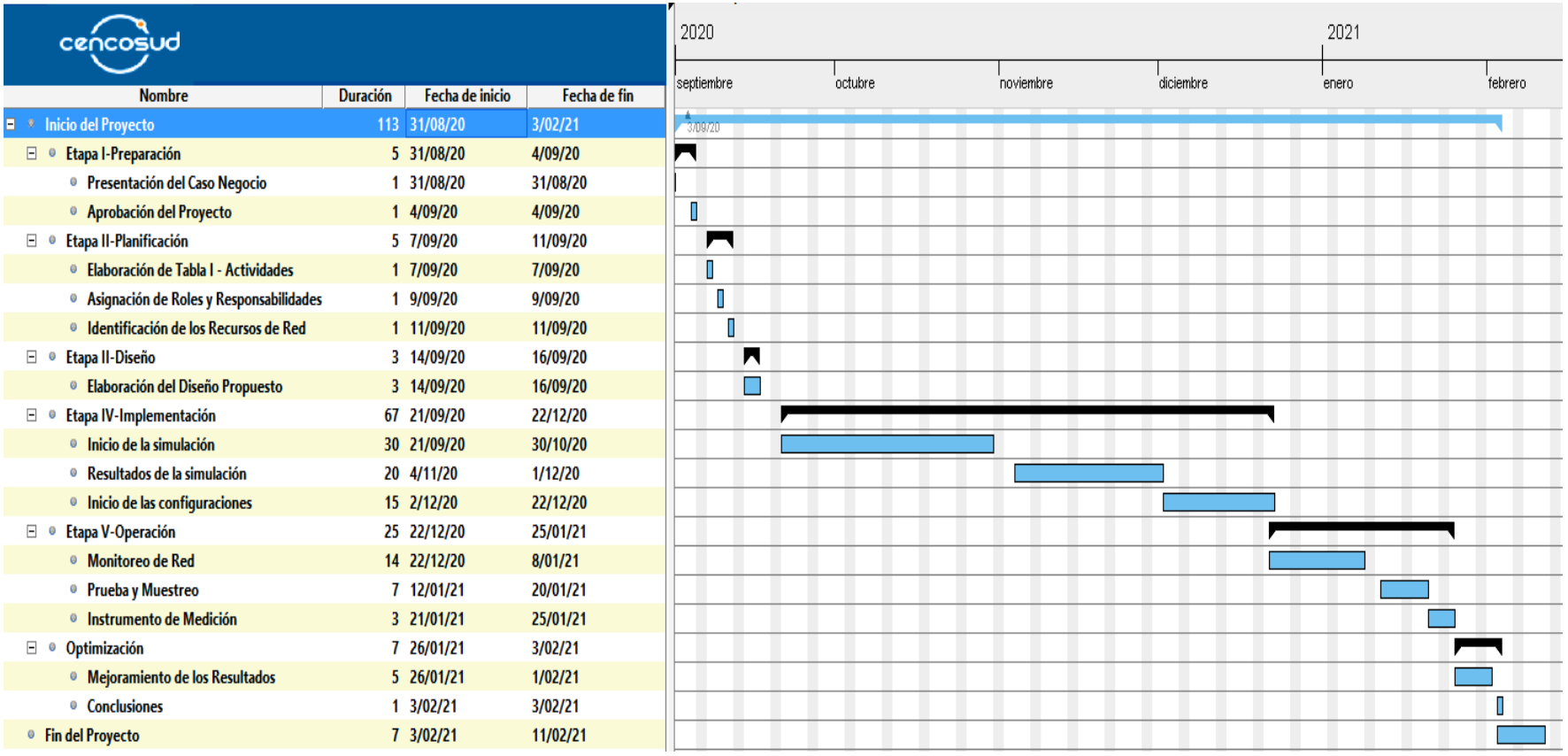
FLUJO DE EGRESOS	
	B
Anual	**Valor (en S/.)**
Mes 1	S/.73,638.33
Mes 2	S/.66,148.33
Mes 3	S/.66,148.33
Mes 4	S/.69,148.33
Mes 5	S/.74,148.33
Mes 6	S/.78,148.33
TOTAL	**S/.430,379.98**

FLUJO EFECTIVO NETO	
	A-B
Anual	**Valor (en S/.)**
Mes 1	S/.26,811.67
Mes 2	S/.58,351.56
Mes 3	S/.65,851.67
Mes 4	S/.80,954.67
Mes 5	S/.84,310.67
Mes 6	S/.90,310.67
TOTAL	**S/406,590.91**

Para calcular el **VAN** (valor actual neto) se considera una tasa de interés de **3%.** A partir de la tasa de interés, se hallará el cálculo del VAN con la siguiente formula: **=VNA (0.3; Sum (Flujo efectivo neto))-350000.00**; que representa el 0.3 de la tasa de interés más la sumatoria de todos lo flujo efectivo neto y al final le restamos la inversión inicial, El resultado es de **S/. 11, 584.36 mil nuevo soles**, lo cual es mayor a cero, Todo **VAN > 0** indica que el proyecto es beneficioso y rentable para la empresa.

VAN (VALOR ACTUAL NETO)	
	Flujo Efectivo Neto
	Valor (en S/.)
Inversión Inicial	**-350000.00**
Mes 1	26,811.67
Mes 2	58,351.56
Mes 3	65,851.67
Mes 4	80,954.67
Mes 5	84,310.67
Mes 6	90,310.67
VAN	**S/11,584.36**

Cronograma de Actividades



Nombre	Duración	Fecha de inicio	Fecha de fin
Inicio del Proyecto	113	31/08/20	3/02/21
Etapa I-Preparación	5	31/08/20	4/09/20
Presentación del Caso Negocio	1	31/08/20	31/08/20
Aprobación del Proyecto	1	4/09/20	4/09/20
Etapa II-Planificación	5	7/09/20	11/09/20
Elaboración de Tabla I - Actividades	1	7/09/20	7/09/20
Asignación de Roles y Responsabilidades	1	9/09/20	9/09/20
Identificación de los Recursos de Red	1	11/09/20	11/09/20
Etapa II-Diseño	3	14/09/20	16/09/20
Elaboración del Diseño Propuesto	3	14/09/20	16/09/20
Etapa IV-Implementación	67	21/09/20	22/12/20
Inicio de la simulación	30	21/09/20	30/10/20
Resultados de la simulación	20	4/11/20	1/12/20
Inicio de las configuraciones	15	2/12/20	22/12/20
Etapa V-Operación	25	22/12/20	25/01/21
Monitoreo de Red	14	22/12/20	8/01/21
Prueba y Muestreo	7	12/01/21	20/01/21
Instrumento de Medición	3	21/01/21	25/01/21
Optimización	7	26/01/21	3/02/21
Mejoramiento de los Resultados	5	26/01/21	1/02/21
Conclusiones	1	3/02/21	3/02/21
Fin del Proyecto	7	3/02/21	11/02/21

Conclusiones

En cuanto al diseño del protocolo SECURE SD-WAN y al desarrollo de cada uno los objetivos específicos, se han determinado las siguientes conclusiones:

- En referencia al primer objetivo específico, recopilar los datos de carga de la empresa Cencosud S.A. para diseñar el protocolo Secure SD-WAN. Se han desarrollado las actividades relacionadas con la recopilación de datos tal como queda demostrado en el CAPITULO III “Planteamiento de la metodología Protocolo Secure SD-WAN” y CAPITULO V “Instrumento de Medición”
- En relación con el segundo objetivo específico, determinar cómo contribuye la capacidad de red para el uso del balanceo de carga en la comunicación de L2L de forma inteligente y segura para la empresa Cencosud S.A. Se ha documentado los resultados como se puede observar en el CAPITULO V “Instrumento de Medición” en la numeración 5.2.1. “Capacidad de Red” y 5.3. “Resultados”.
- Finalmente, corresponde al último objetivo específico, realizar el monitoreo de los enlaces para medir el rendimiento en el balanceo de carga en la comunicación de L2L de forma inteligente y segura para la empresa Cencosud S.A. Se ha descrito todas las actividades de monitoreo, tal como se aprecia en los CAPITULO IV “Desarrollo de la Metodología Protocolo Secure SD-WAN” en los numerales 4.2.5. “Etapa de Operación” y CAPITULO V “Instrumento de Medición” en la numeración 5.3. “Resultados”.

Recomendaciones

- La implementación del Diseño del Protocolo de Secure SD-WAN para garantizar el balanceo de carga en la comunicación de L2L de forma inteligente y segura para la empresa Cencosud S.A, deberá ser apoyada desde la alta dirección para asignar a los especialistas idóneos, para una administración eficiente eficaz de la red en el futuro.
- Se deberá mantener al personal en constante capacitación para manejar la escalabilidad de la nueva solución de Secure SD-WAN.
- Se deberá mejorar las políticas de monitoreo continuo para cada control del tráfico de red que permitirá asegurar la distribución y control de los recursos de capacidad de red.
- Se deberá respetar el cronograma de mantenimiento preventivo para mantener el estado de la red y asegurar su operación de forma eficaz y segura de esta manera se asegurará la eficacia y eficiencia de las operaciones.

Lista de Anexos

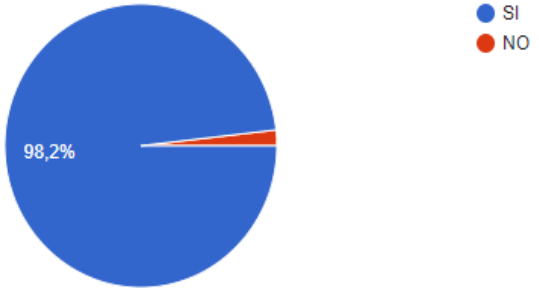
Anexo 1: Encuesta Sobre el acceso a los sistemas informáticos y velocidad de red

Tipo de Usuario:

Encuestados: 56 personas

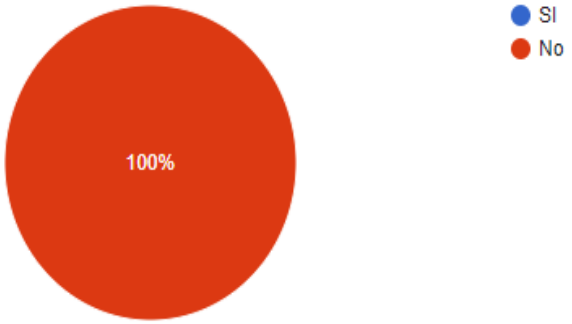
1. ¿En la actualidad trabajan de manera eficiente con los sistemas informáticos?

56 respuestas



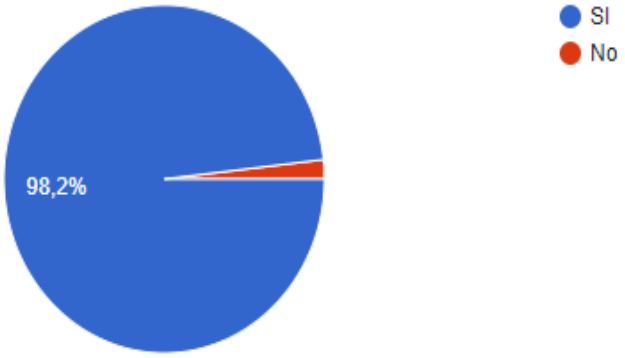
2. ¿Presentan problemas de velocidad de red sobre el uso de los sistemas informáticos?

56 respuestas



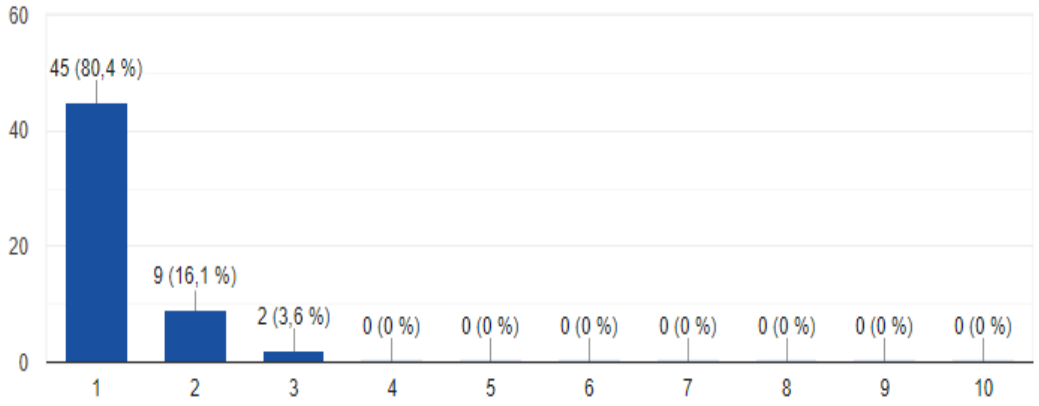
3. ¿Trabajan de forma ágil y de manera eficiente con la conexión de los sistemas informáticos?

56 respuestas



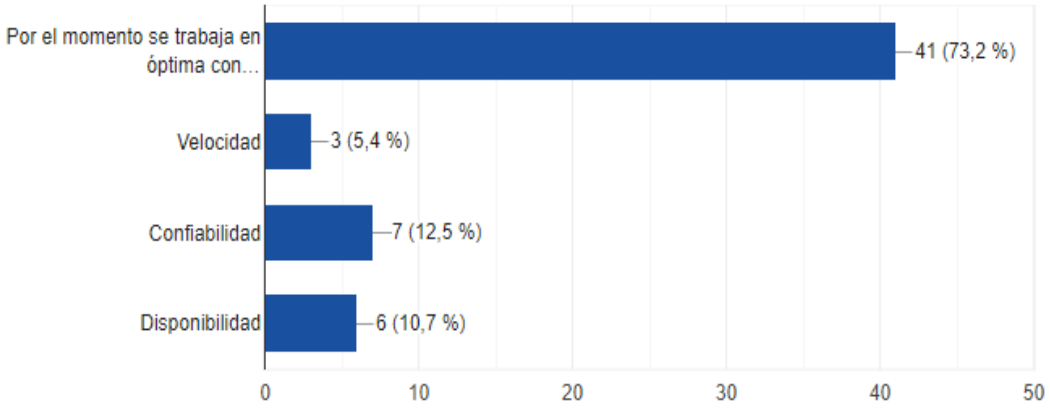
4. ¿Del 1 al 10 que tan lenta es la conexión con los sistemas informáticos?

56 respuestas



5. ¿Qué quisiera usted que se mejore en el acceso a la red y a los sistemas informáticos?

56 respuestas



Anexo 2: Formato de bitácora de hechos relevantes

AÑO	2021

	CENCOSUD S.A.							
N°	**Registrado por (Operador TAC)**	**Reportado por**	**Fecha y Hora de Inicio**	**Fecha y Hora de Solución**	**Tiempo de evento**	**Nro Ticket**	**¿Programado?**	**Indisponibilidad del Servicio**
1	Juan Espinoza	Monitoreo	20/03/2021 00:00	20/03/2021 02:00	2:00:00	17689	NO	SI

Servicio	**Categoría**	**Sub-Categoría**	**Descripción del Problema**	**Solución**	**Causa Raiz / Motivo**	**Grupo Resolutor (resuelve incidencia)**	**Responsable de la solución**	**Estado Ticket**
L2L	Medio_Fisico	T.I._Mantenimiento	Se realizarán trabajaos de reposición y fusión de la FO	Reposición de FO	Factor Externo	Infraestructura_Red	I. Echegaray	Asignado

Anexo 3: Formato de mantenimiento preventivo

INFORME DE MANTENIMIENTO PREVENTIVO

Departamento: Telecomunicaciones
De : Área de Networking
Asunto : Mantenimiento Preventivo

---

1. INTRODUCCIÓN

El presente informe detalla las acciones realizadas para en el mantenimiento preventivo.

2. VERIFICACION DE EQUIPOS Y SERVICIO

El día dd/mm/aaaa nos comunicamos con el cliente **XXXX (Contacto)** para realizar pruebas sobre el servicio de xxxx circuito **XXXX.**

2.1. **Verificación de equipos: modelo x.x.x.x serie xxxx (Anexo x)**

Nro.	Item	SI	NO
	Adecuado estado de instalaciones y conexiones físicas		
1.	Medición del Cable de alimentación eléctrica	X	
2.	Medición de la calidad del Patch Cord de cobre	X	
3.	Medición de la calidad de enlace de Fibra Óptica		
4.	Limpieza y mantenimiento de los componentes ópticos de los enlaces de transmisión de datos (L2L)	X	
	Revisión de hardware/software del router		
5.	Errores en Interfaz		X
6.	Negociación de las interfaces de red: 100 FULL	X	
7.	Firmware actualizado (versión: _____)	X	
8.	CPU del router (<50%)	X	
9.	RAM del router cuenta con espacio disponible (mín. 30%)	X	
10	FAN del router se encuentran operativo	X	
	Diagnostico:		
11	Requiere cambio de toma o cable eléctrico		X
12	Requiere cambio del enlace de FO		X
13	Requiere cambio del enlace de cobre		
14	Requiere cambio de equipamientos		X

Atentamente,

Departamento de Telecomunicaciones
CENCOSUD S.A.

Anexo 4: Datasheet de Secure SD-WAN

PRODUCT OFFERINGS

FortiGate

SD-WAN Branch Offices	Fortigate 30E	Fortigate 50E	Fortigate 100E	Fortigate 200E	Fortigate 300E
Use Case					
Type	Remote Office/Home	Small Branch	Medium Branch	Large Branch	Large Branch
Performance					
Unrestricted Bandwidth	Fortinet Secure SD-WAN offers unrestricted bandwidth unlike other SD-WAN vendors				
IPSEC VPN Throughput	4.4 Gbps	6.5 Gbps	6.5 Gbps	11.5 Gbps	13 Gbps
Application Control Throughput	990 Mbps	1.8 Gbps	1.8 Gbps	2.2 Gbps	13 Gbps
Max Concurrent Connections	700,000	700,000	1,500,000	1,500,000	3,000,000
Threat Protection Throughput	600 Mbps	700 Mbps	900 Mbps	1 Gbps	3 Gbps
SSL Protection Throughput	310 Mbps	630 Mbps	715 Mbps	1 Gbps	4 Gbps
Connectivity					
Total Interfaces	4	6	8	14	26
Max FortiLink Ports	1	2	2	2	2
10GE	-	-	-	2	2
Dual Power Supply	-	-	✓*	✓	✓
Variants					
Built-in	3G/4G, WiFi	WiFi, Storage	Bypass, Storage	Storage	Storage
Form Factor	Desktop	Desktop	Desktop	1RU	1RU

Use Case	Offering Name	Support	Priority Access To Level 2 Support	Content Protection With AV & Cloud Sandbox	Web & Application Access Protection	Vuln. And Device Protection (Iot/Ot)	Compliance Monitoring Tools	SD-WAN Management & Orchestration	Network & Security Cloud Management
WAN Edge	360 Protection Bundle	24 × 7	✓	✓	✓	✓	✓	✓	✓

	Features	Description
FortiOS — SD-WAN	Application Identification & Control	5000+ Application signatures, First packet Identification, Deep packet Inspection, Custom application signatures, SSL decryption enabled, TLS1.3 with mandated ciphers and deep inspection.
	SD-WAN (Application aware traffic control)	Granular application policies, Application SLA based path selection, Dynamic bandwidth measurement of SD-WAN paths, active/active and active/standby forwarding, overlay support for encrypted transport, Application session-based steering, probe-based SLA measurements
	Advanced SD-WAN (WAN remediation)	Forward Error Correction (FEC) for packet loss compensation, packet duplication for best real-time application performance, Active Directory integration for user based SD-WAN steering policies, per packet link aggregation with packet distribution across aggregate members
	SD-WAN deployment	Flexible deployment – hub-to-spoke (partial mesh), spoke-to-spoke (full mesh), Multi-WAN transport support

Referencias Bibliográficas

Banco Scotiabank del Perú. (2019 de Julio de 2019). *Scotiabankfiles*. Obtenido de https://scotiabankfiles.azureedge.net/scotiabank-peru/PDFs/semanal/2019/julio/20190704sem_es.pdf

Cisco System. (2018). *Estudios de caso BGP*. Obtenido de https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html

Cisco System. (2019 de Septiembre de 2019). *Cisco solutions*. Obtenido de Obtenido de la página de partners de la corporación internacional Cisco System; La red de SD-WAN:: https://www.cisco.com/c/es_pe/solutions/enterprise-networks/sd-wan/what-is-sd-wan.html

Cisco System. (16 de Mayo de 2019). *Guía de Configuración IKE*. Obtenido de https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ikevpn/configuration/xe-16-11/sec-ike-for-ipsec-vpns-xe-16-11-book/sec-key-exch-ipsec.html

Erazo, P. F. (2016). *Repositorio Puce*. Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/13491/Tesis%20Pablo%20Erazo%20Guerra.pdf?sequence=1&isAllowed=y

Espinoza Chipane. (Febrero de 2018). *Implementación de una red privada virtual en supermercados Mass*. Obtenido de Obtenido de Administracion Estratégica: http://repositorio.autonoma.edu.pe/bitstream/AUTONOMA/487/2/ESPINOZA%20CHIPANE%20CESAR%20RENATO.pdf

Fortinet. (2019). *Solución Secure SD-WAN*. Obtenido de https://www.fortinet.com/lat/products/sd-wan

Fortinet INC. (2019). *Libreria de Fortinet INC*. Obtenido de Obtenido de docuemntos Fortinet: https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/19246/sd-wan

Fortinet INC. (2019). *SD-WAN_6.2_Study_Guide.* Sillicon Valley: Fortinet Training.

Fortinet INC. (27 de Agosto de 2020). *Guía de Estudio NS4 SD-WAN*. Obtenido de SD-WAN_6.2_Study_Guide-Online.pdf

Fortinet INC. (2020). *Repocitorio de la academia de Fortinet*. Obtenido de Obtenido de la gía de estudio SD-WAN: https://www.fortinet.com/support-and-training/training/network-security-expert-program.html

Gartner INC. (2020). *Tendencia SD-WAN 2020*. Obtenido de https://ipmoguide.com/sd-wan-trends-2020-tendencias/

ITIL Foundation. (18 de Julio de 2019). *Aprende cómo distribuir mejro las responsabilidades con la Matriz RACI*. Obtenido de Obtenido de Blog Rockcontent: https://rockcontent.com/es/blog/matriz-raci/

Lacnic INC. (04 de Mayo de 2018). *Curso Oficial de Border Gateway Protocol*. Obtenido de Obtenido de la escuela de Lacnic Latinoamerica: https://www.lacnic.net/innovaportal/file/2621/1/bgp-panama-lacnic29.pdf

Martel Velasquez. (2018). *Repositorio UPC*. Obtenido de Obtenido de la Escuela de Sistema de la información: https://repositorioacademico.upc.edu.pe/handle/10757/625693

Martel, V. R. (2020). *Repositorio Academico UPC*. Obtenido de Diseño de una red de comunicación VPN:

https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/625693/Martel_Vv.pdf?sequence=1&isAllowed=y

Ostec. (18 de Julio de 2018). *Principales conceptos y modelo de funcionamiento de SD-WAN*. Obtenido de https://ostec.blog/es/seguridad-perimetral/sd-wan-conceptos-funcionamiento

Pursell, Shelley. (27 de Febrero de 2020). *Matriz RACI: Asignar Responsabilidades*. Obtenido de https://blog.hubspot.es/marketing/matriz-raci

Vásquez, V. (2012). *Implementación de una RED PRIVADA VIRTUAL*. Obtenido de http://tesis.usat.edu.pe/bitstream/20.500.12423/1619/1/TL_AmeneroVasquezVirgilio.PDF